VIEW Certified Configuration Guide

Cisco

2100/2500/4400/5500/7500/8500 Series WLC (Wireless LAN Controller),

WiSM (Wireless Services Module), WiSM2, WLC Module, WLC SW for SRE, 3750G Integrated WLC, and Virtual Controller

with 60x, AP801, AP802, 104x, 113x, 114x, 1121, 122x, 123x, 124x, 125x, 126x, 13xx, 152x, 155x, 160x, 260x, 350x, 360x APs

1725-86192-000 Rev: AA
August 2013

Copyright Notice

© 2009-2013 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Contact Information

US Location
800-775-5330

Spectralink Corporation
1765 W. 121st Avenue
Westminster, CO 80234

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Langmarksvej 34
8700 Horsens

infodk@spectralink.com

Contents

Introduction 5

Certified Product Summary 5
Known Limitations 7
Spectralink References 7
Specific Documents 8
Product Support 9

Chapter 1: Configuration for Wi-Fi Standard QoS or CCXv4 Operation 10

Overview 10
Network Topology 11
Configuring a New Controller Starting from Factory Defaults 12
Connecting to the Controller Via a Browser 12
Installing Software 13
Controller Setup 14
Connecting APs 17
Defining a RADIUS Server 19
AP Configuration 20
Configuration for handsets running in 802.11b, b/g mixed mode, g only mode in 8020/8030 handsets or 2.4 GHz in 84-Series handsets 21
Configuring 802.11n 26
Configuration for handsets running in 802.11a mode in the 8020/8030 handsets and using the 5 GHz radio in the 84-Series handsets 27
Configuring 802.11n: 32
Setting up the SSID 35
Setting up the EDCA parameters profile 41
Configuration for handsets running in 802.11a mode mode in 8020/8030 handsets or 5 GHz in 84-Series handsets 41
Configuration for handsets running in 802.11b/g mode, 802.11b and b/g mixed mode, or 802.11 g only mode in 8020/8030 handsets or 2.4 GHz in 84-Series handsets 41

Chapter 2: Configuration for SVP Operation 42

Introduction 42
Network Topology 42
Configuring a New Controller Starting from Factory Defaults 43
Connecting to the Controller via a Browser 44
Installing Software 45
Controller Setup 46
Connecting APs 49
Defining a RADIUS Server 51
AP Configuration 53
Configuration for handsets running in 802.11b & b/g mixed and g only mode 53
Configuring 802.11n 56
Configuration for handsets running in 802.11a mode 57
Configuring 802.11n: 60
Setting up the SSID 62
Setting up the EDCA parameters profile 68
Configuration for handsets running in 802.11a mode mode in 8020/8030 handsets 68

Configuration for handsets running in 802.11b/g mode, 802.11b and b/g mixed mode, or 802.11 g only mode in 8020/8030 handsets 68

Introduction

Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between Spectralink 8440/8441/8450/8452/8453 and 8020/8030 Wireless Telephones and WLAN infrastructure products.

The products listed below have been tested in Spectralink's lab and have passed VIEW Certification.

Certified Product Summary

Manufacturer:	Cisco Systems: www.cisco.com			
Certified products:	Controllers: 2100, 2500, 4400, 5500 Series WLC (Wireless LAN Controller) 3750G Integrated WLC, WLC Module, WiSM (Wireless Services Module), WiSM2, Virtual Controller	APs: 60x AP801 AP802 104x 1121 113x	114x 122x 123x 124x 125x 126x	13xx 155x 160x 260x 350x 360x
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)			
Security:	None, WEP, WPA-PSK, WPA2-PSK, WPA2-Enterprise (EAP-FAST and PEAPv0/MSCHAPv2) with CCKM (Cisco Centralized Key Management)** and OKC			
QoS:	Wi-Fi Standard for Spectralink 8440/8441/8450/8452/8453 and 8020/8030 SVP for Spectralink 8020/8030			
AP and WLC software versions approved:	6.0.202.0 for AP801, 113x, 114x, 1121, 122x, 123x, 124x, 125x, and 13xx Aps with 2100, 4400, 3750G, 5500, WiSM, WLC Module 7.0.220.0 for 60x, AP801, AP802, 104x, 1121, 113x, 114x, 122x, 123x, 124x, 125x, 126x, 13xx, 155x and 350x Aps with 2100, 2500, 4400, 3750G, 5500, 7500, WLC SW for SRE, WiSM, WiSM2			

	7.2.110.0 and 7.3.101.0 for 60x, AP801, AP802, 104x, 113x, 114x, 124x, 125x, 126x, 155x, 260x, 350x and 360x with 2500, 5500, WiSM2, WLC SW for SRE 7.4.110.0 for 60x, 70x, AP801, AP802, 104x, 113x, 114x, 124x, 125x, 126x, 155x, 160x, 260x, 350x, and 360x with 2500, 5500, 7500, 8500, WiSM2, WLC SW for SRE, Virtual Controller 7.5.102.0 for 60x, 70x, AP801, AP802, 104x, 113x, 114x, 124x, 125x, 126x, 155x, 160x, 260x, 350x, and 360x with 2500, 5500, 7500, 8500, WiSM2, WLC SW for SRE, Virtual Controller			
Network topology:	Switched Ethernet (recommended)			
Handset models tested:*	*Spectralink 8440/8441/8450/8452/8453 Wireless Telephone*			
Handset radio mode:	802.11b	802.11b/g	802.11bgn	802.11a & 802.11an
Meets VIEW minimum call capacity per AP:	8 calls	8 calls	8 calls	10 calls
Handset models tested:	*Spectralink 8020/8030 Wireless Telephone*			
Handset radio mode:	802.11b & b/g mixed. 802.11 g only		802.11a	
Meets VIEW minimum call capacity per AP:	6 (Wi-Fi Standard QoS)** 8 calls (SVP)		8 (Wi-Fi Standard QoS) ** 12 calls (SVP)	

*Spectralink handset models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as “Spectralink Wireless Telephones”, “phones” or “handsets”. The 8440, 8441 (8440 with personal alarm hardware), 8450 (with 1D bar code reader), 8452 (with 1D and 2D bar code reader), and 8453 (8452 with personal alarm hardware) handsets will be referred to collectively as the 84-Series handsets.

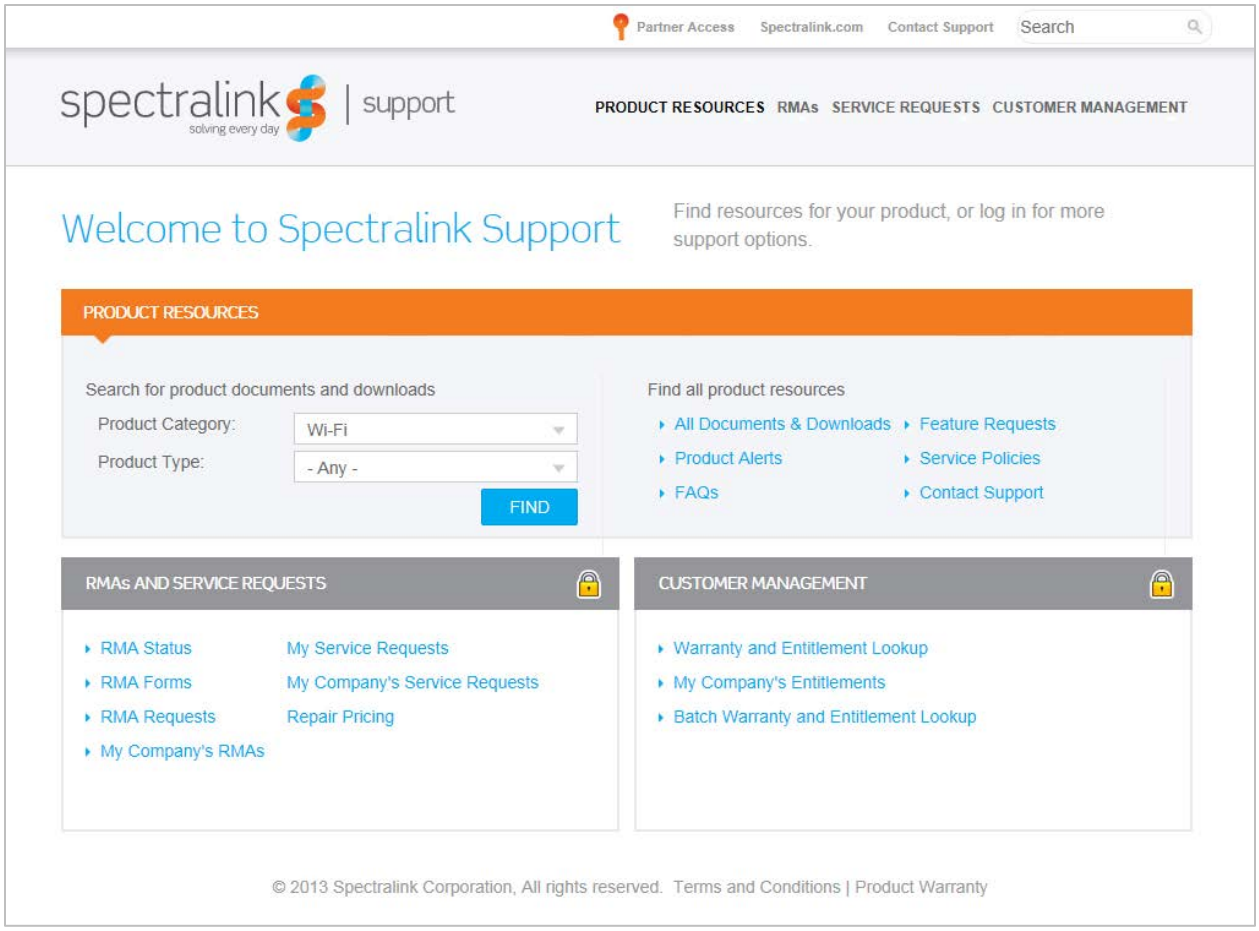
** Only Release 3.0 capable Spectralink 8020/8030 handsets support WPA2-Enterprise, Wi-Fi Standard QoS, and CCXv4 (Cisco Compatible Extensions). Release 3.0 capable handset types connect to PBX's that support IP telephony. Release 3.0 capabilities are not available for Spectralink 8020/8030 handsets connecting to PBXs using the TDM protocol through a Spectralink Telephony Gateway (handset type 30 on the 8020/8030).

Known Limitations

- Heavy multicast, broadcast or push-to-talk (PTT) traffic may impair voice quality on 6.0 and 7.0 versions.
- When Spectralink Voice Priority (SVP) is enabled for Spectralink 8020/8030 in the EDCA parameters setting, the 802.11n capabilities will be disabled on that radio when using Cisco 6.0 software versions (see Section 1: Configuring for SVP Operation → AP Configuration). It is therefore recommended to deploy handsets using SVP on a different radio than 802.11n clients.
- Fast Transition Roaming (802.11r) is not yet supported by the handsets
- Multicast by VLAN is not compatible with the PTT feature in the handsets.
- When using 7.0 versions, 5 GHz radio, 1142 AP's, and 80xx handsets, CSD must be disabled on the AP's.
- When using 1142 AP's, A-MPDU aggregation must be disabled if 11n is enabled
- A-MSDU aggregation must be disabled if 11n is enabled
- In the controller software versions considered in this document, there is an issue related to band steering that can cause slow roaming on the 2.4 GHz band in the 84-Series handsets when both radios are active in the handset.
- In the WMM/QoS mode, it is important to use the Static CAC Method rather than the Load Based CAC Method.
- Cisco WLC Version 7.4.100.0 is not compatible with Spectralink handsets.
- The handsets have not yet been tested in the presence of active 802.11ac clients.

Spectralink References

All Spectralink documents are available at http://support.spectralink.com.



To go to a specific product page:

Select the Product Category and Product Type from the dropdown lists and then select the product from the next page. All resources for that particular product are displayed by default under the All tab. Documents, downloads and other resources are sorted by the date they were created so the most recently created resource is at the top of the list. You can further sort the list by the tabs across the top of the list to find exactly what you are looking for. Click the title to open the link.

Specific Documents

For the Spectralink 8020/8030 Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 8020/8030 Wireless Telephones.* This white paper covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For the Spectralink 84-Series Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 84-Series Wireless Telephones* for detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

These two white papers identify issues and solutions based on Spectralink's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

The *Spectralink 84-Series Wireless Telephone Administration Guide* provides a comprehensive list of every parameter available on Spectralink 84-Series Wireless Telephones.

The *Spectralink 84-Series Deployment Guide* is your essential reference for provisioning and deploying Spectralink 8400 handsets in any environment.

The *Web Configuration Utility User Guide* explains how to use a web browser to configure the Spectralink 84-Series handsets on a per handset basis.

The *Spectralink 8020/8030 Wireless Telephone Handset Administration Tool* document explains how to use a software interface to configure the handsets.

Product Support

Note: Converting autonomous APs to Lightweight mode

This document does not cover the steps involved in converting autonomous APs to Lightweight mode such that they can be controlled by the Cisco WLCs.

Please contact Cisco's Customer Support at www.cisco.com for instructions on this procedure. Once the APs are converted, this document can be used to provision APs.

Note: RADIUS server configuration

This document does not cover the steps involved to configure a RADIUS server required for using WPA2-Enterprise or Cisco FSR security types.

- Installation and configuration guides for Cisco Wireless LAN Controllers can be found on Cisco's website.
- To convert Autonomous APs to Lightweight mode, go to: http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html
- For other assistance, contact either Cisco's or Spectralink's customer service at: www.cisco.com or www.Spectralink.com

Chapter 1: Configuration for Wi-Fi Standard QoS or CCXv4 Operation

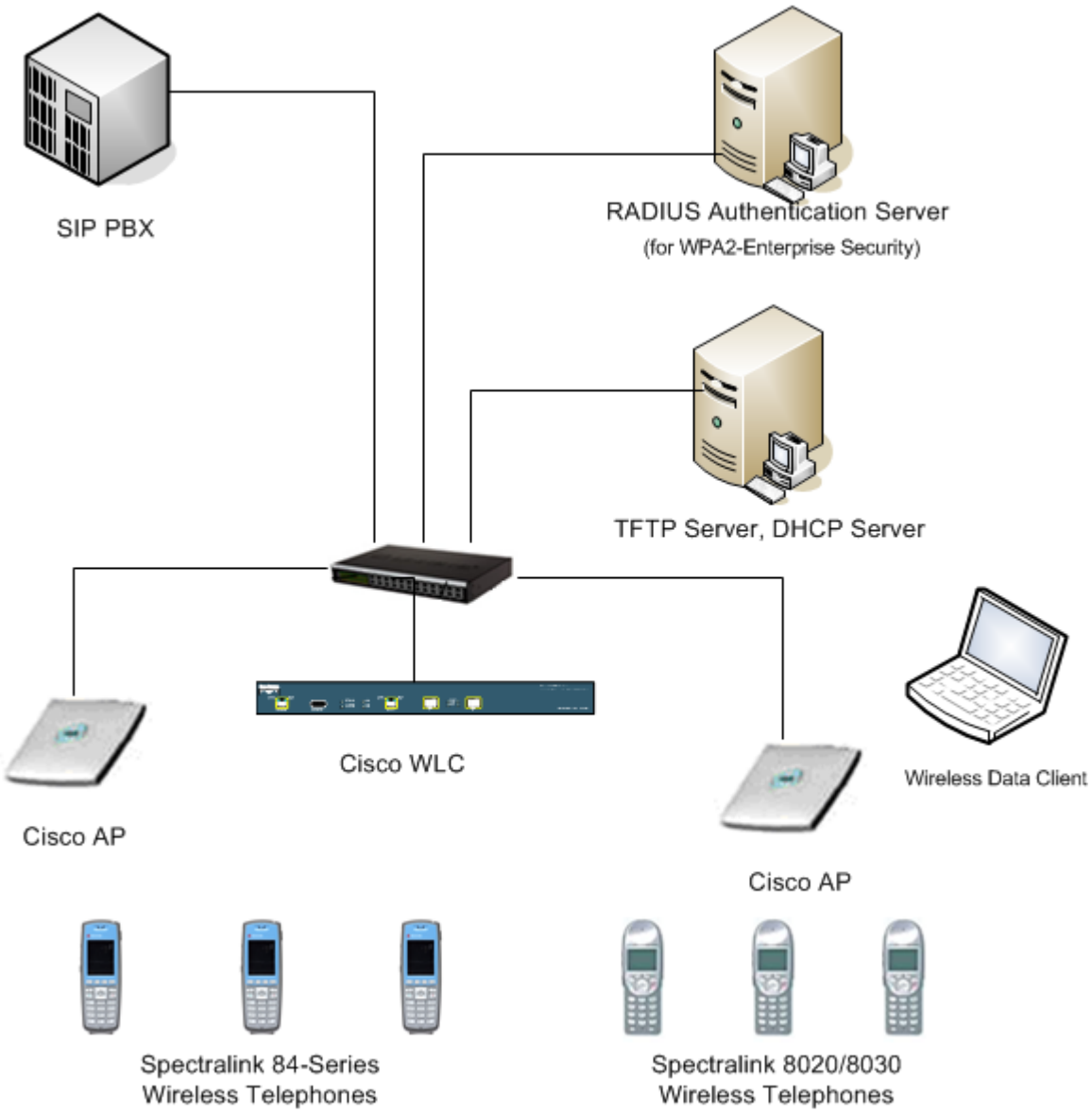
Overview

Spectralink 8020/8030 handsets can be configured with Wi-Fi Standard QoS from the WLAN Settings menu using either the Custom or CCX selection.

- If the Custom menu is selected, QoS Wi-Fi Standard is selected from the QoS submenu.
- If the CCX menu is selected from the WLAN Settings menu, Wi-Fi Standard QoS is used automatically without any further menu selections.

Spectralink 84-Series handsets only support Wi-Fi Standard QoS. The handsets are compatible with both networks configured with CCX (Cisco Compatible Extensions) and networks that are not configured with CCX, but they have not been CCX certified.

Network Topology



Note: Example configuration shown

This configuration is not applicable to all customer environments.

Configuring a New Controller Starting from Factory Defaults

Initial provisioning of the controller is done via the command line interface (CLI).

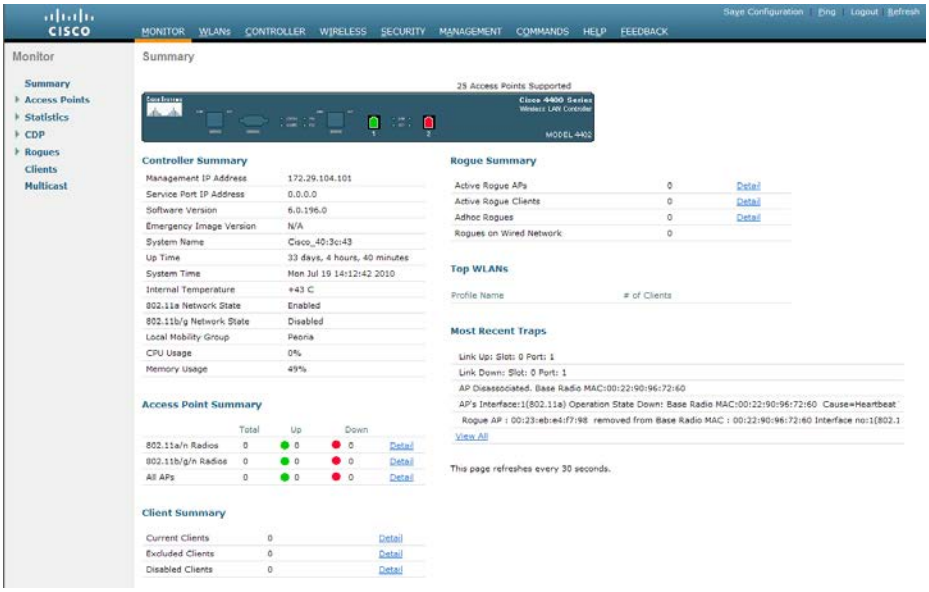
1. Connect a null modem serial cable between the console port of the controller and the serial port of a PC.
2. Open a terminal program, such as Hyper Terminal, and configure the port settings to 9600 baud, no parity, 8 data bits and 1 stop bit.
3. Power-on the controller. Status of the controller's boot process will appear as the controller is powering up. Once the controller is running, it will prompt you to run the Startup Wizard.
4. The Startup Wizard provides for an easy means to perform initial controller setup and provisioning. Refer to the Installation and Startup Guide for the Cisco 5500 Series WLC, or other appropriate controller, found at Cisco's website. This document contains a detailed explanation of using the Startup Wizard for the 5500: http://www.cisco.com/en/US/docs/wireless/controller/5500/install/guide/ctrl5500.htmlOnce the controller has been configured via the Startup Wizard, the remaining configuration can be configured through the switch-web interface using a Web browser (Cisco recommends using MS IE 6.0+).
5. If necessary, the controller can be reset to factory defaults. To reset the WLC to factory default, you must reboot, then type Recover-config at the CLI. This only works before the first time a user logs in via the console.

A few advanced commands must be set from the command line interface after the rest of the controller has been configured. These are noted in the instructions below.

Connecting to the Controller Via a Browser

1. Connect to the WLC by pointing your internet browser to the URL: https<IP_Addr> (where <IP_Addr> is the IP address of the management interface of the WLC).
2. Click the **Login** prompt. The default **User Name** and **Password** is **admin**.

Once logged in properly, a page similar to the one below displays.



Installing Software

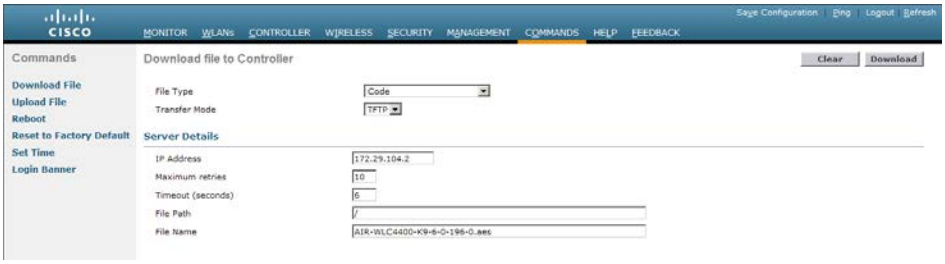
1. To check the installed version of software, listed in the Product Summary, click **Monitor** from the main menu.
2. In the navigation pane, click **Summary**. The heading labeled Software Version shows the current software version.
3. Download the appropriate software for your model of controller from the Cisco website.
4. Set up a Trivial File Transfer Protocol (TFTP) server running on a PC to download the file to the controller.
5. From the main menu, click **Commands**.
6. In the navigation pane, click **Download File**.
7. Fill in the download parameters:
   a. For **File Type**, select **Code**.
   b. For **TFTP Server**, type in the IP Address of the TFTP server.
   c. Add the **File Path** (this is the path in the TFTP server's root directory and not the system path where the TFTP server is located) and **File Name** of the firmware file to download.

Note

The example simply uses the /designator for the root TFTP directory.

8 Point the TFTP server to the code.

9 Click **Download** and allow a few minutes for the download to complete.



10 Reboot the Controller.

Controller Setup

The initial setup of the controller is shown below.

Note: Example only

The setup instructions outlined in this document are for the configuration shown in the diagram only. Your configuration may differ, and the appropriate adjustments must be made.

Note: The WLC will provision the APs

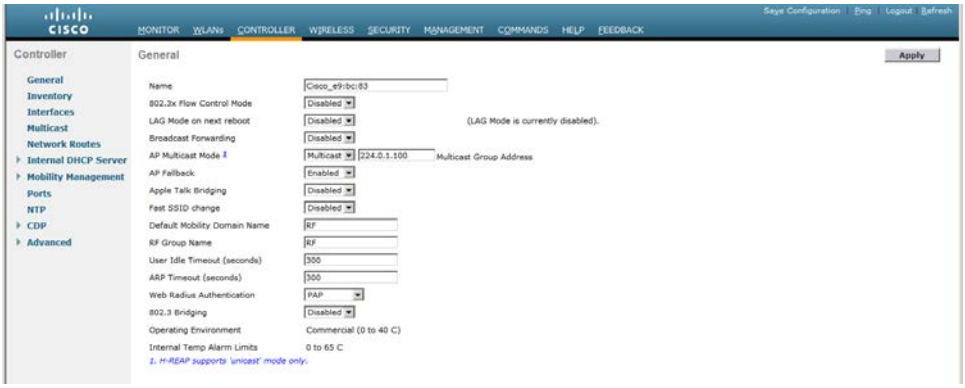
It is not necessary to configure each AP individually. The WLC is capable of provisioning the APs.

1 From the main menu, click **Controller**.

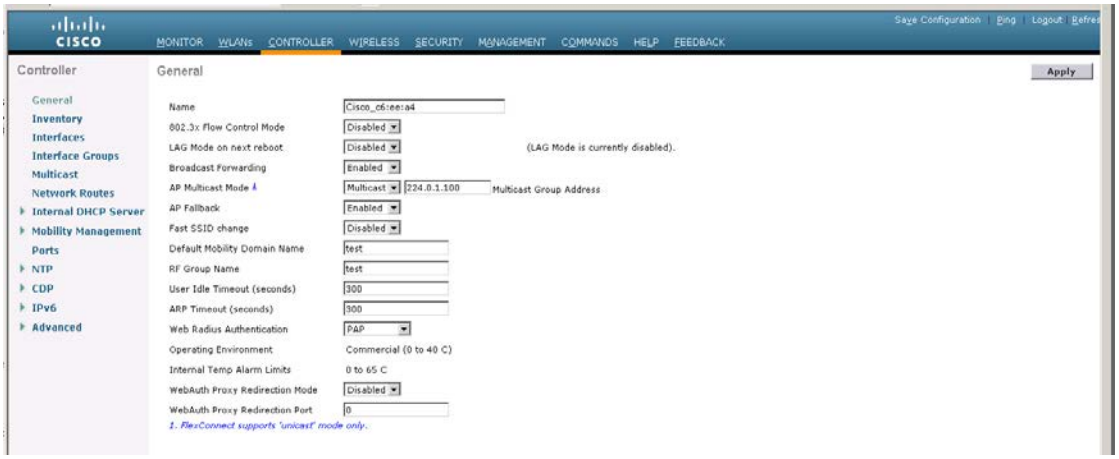
2 Set the AP Multicast Mode to Multi**c**ast and enter a multicast IP address that is currently not being used on your network for the Multicast Group Address.

3 Click the **Apply** button.

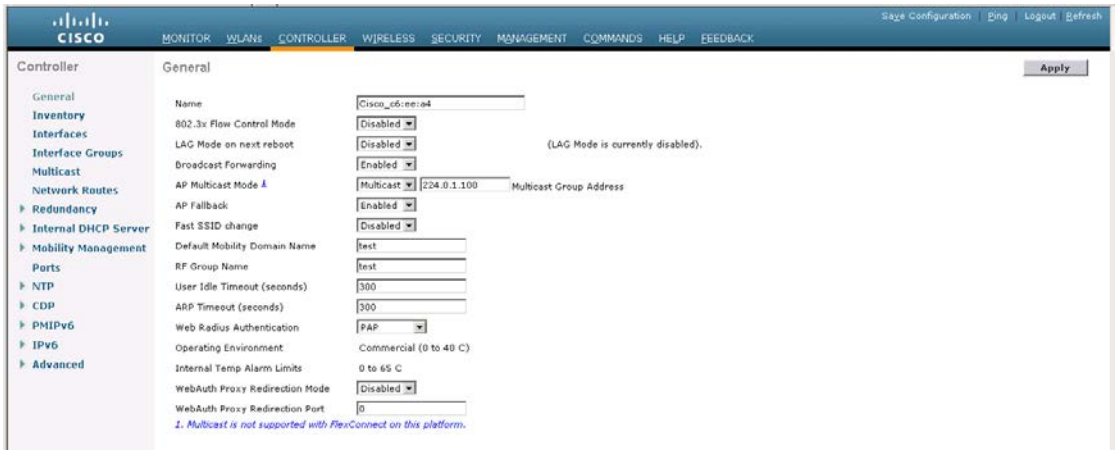
Cisco 6.0 versions:



Cisco 7.0 and 7.2:



Other versions:

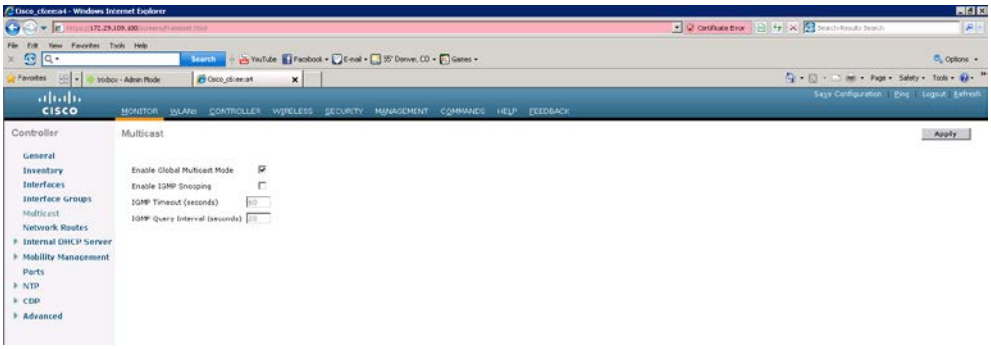


4 Click **Multicast** from the options on the left side of the screen

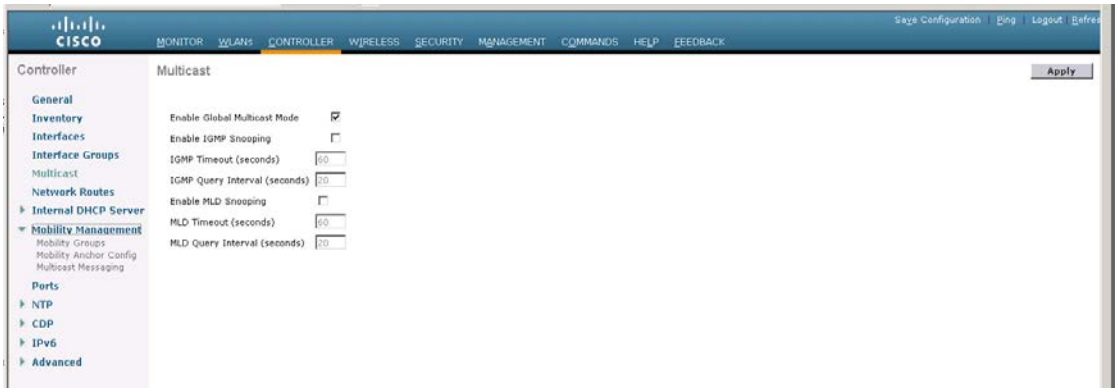
5 Select **Enable Global Multicast Mode** checkbox

6 Click the **Apply** button.

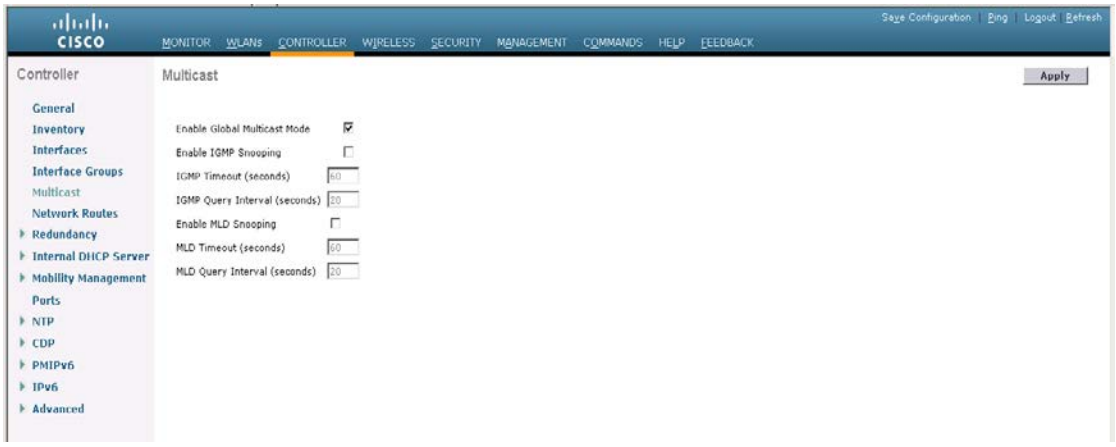
Cisco 6.0 versions:



Cisco 7.0 and 7.2 versions:



Other versions:



7 Click **Save Configuration**.

Connecting APs

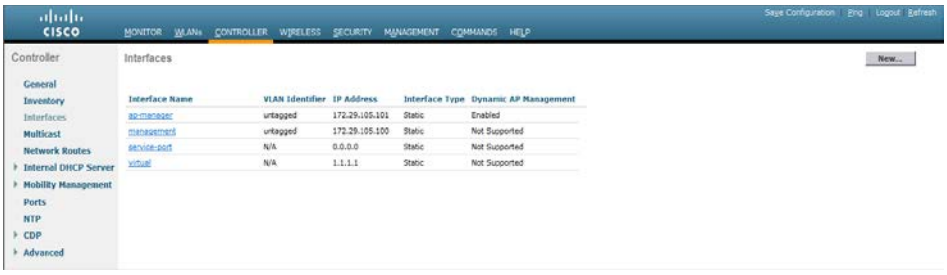
As the APs are connected to the network, they should automatically find the controller via the CAPWAP discovery algorithms. The Dynamic Host Configuration Protocol (DHCP) server will assign each AP an IP address.

Admin Tip: DHCP server

You can configure a DHCP server to run on a remote PC for a small deployment. However, for large-scale deployments, an enterprise-grade DHCP server must be used.

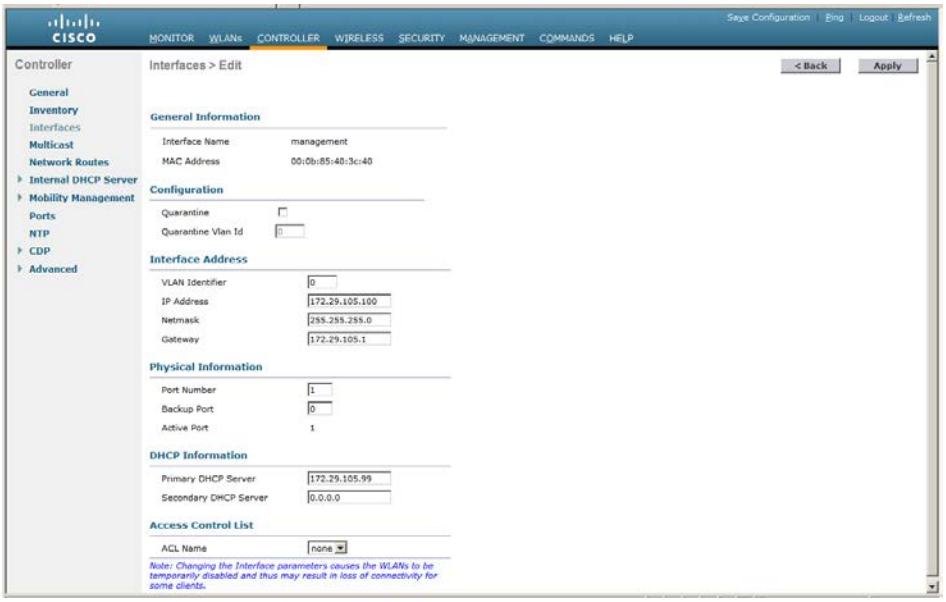
The **ap-manager** and **management** interfaces' configuration should include the DHCP server you have configured. Alternately, you can configure the DHCP server internally on the controller to hand out leases to the connected clients. (Note: The WLC's DHCP server does not lease addresses to the AP.) The instructions for doing so are included at the end of this document.

1. From the main menu, click **Controller**.
2. In the navigation pane, click **Interfaces**. Verify that the proper IP addresses are assigned to the interfaces.
3. Under Interface Name click **management**. Note: the screenshot is from a Cisco 4400. The 2100 does not contain a service-port interface. The 5500 does not contain an ap-manager interface. 7.3 and later versions provide redundancy management and redundancy port entries. If the interface is not present on the model being configured, no values need to be entered.

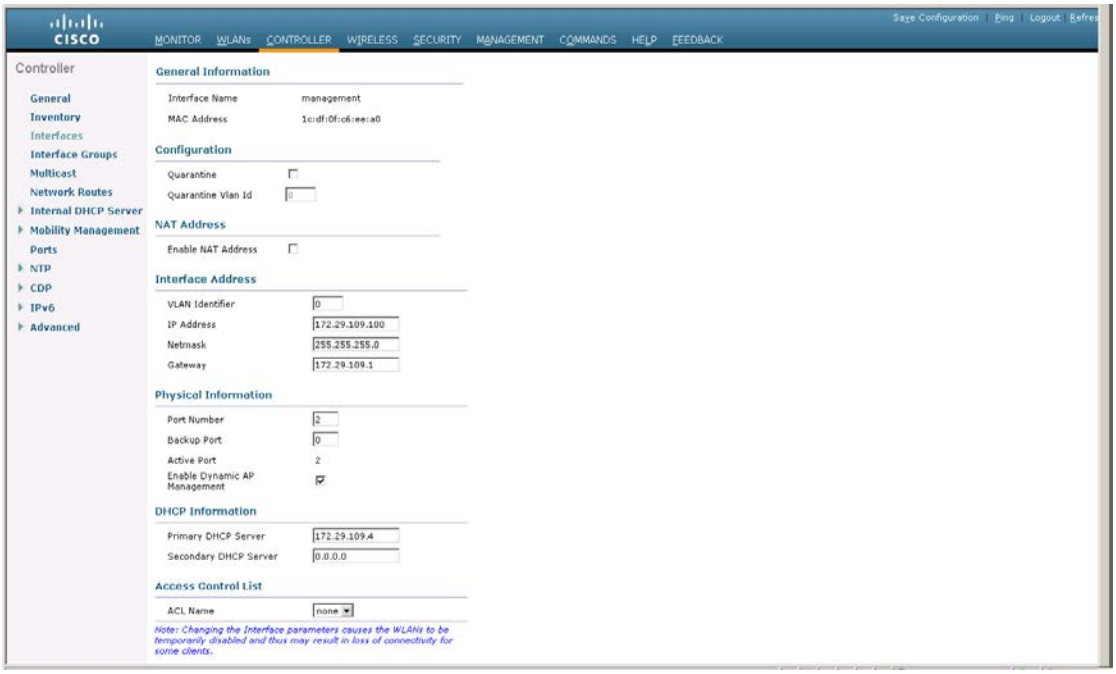


4. Under DHCP Information, enter the IP address of the Primary DHCP Server.
5. Repeat this step for the ap-manager interface, if present on the model configured.
6. Click the **Apply** button and save the changes.

Cisco Controllers other than the 5500:



Cisco 5500:



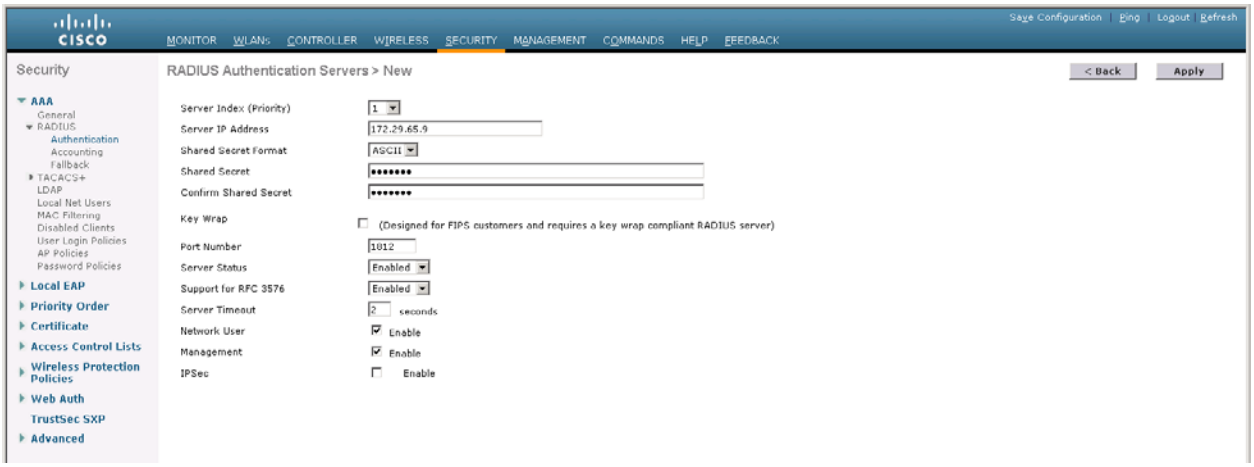
7 Under service-port, (if present), enter a valid IP Address and Netmask in a different subnet than the management interface.

8 Click the **Apply** button and save the changes.

Defining a RADIUS Server

If it is desired to use WPA2-Enterprise security, it is necessary to define a RADIUS server.

1. From the main menu, click **SECURITY**.
2. Expand RADIUS in the left pane.
3. Click **Authentication**.
4. Click **New**… in the right hand corner of the screen.
5. Enter the IP Address of the RADIUS server in the Server IP Address field.
6. Enter the Shared Secret from the RADIUS server in the Shared Secret and Confirm Shared Secret fields.



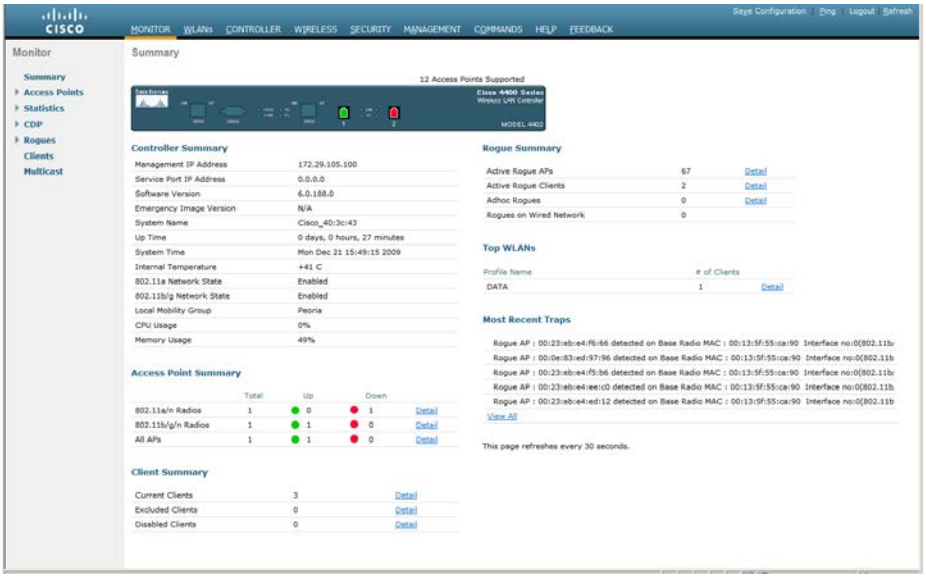
7. Click **Apply**. The RADIUS server will now be available for selection in the WLANs menu security screens.

AP Configuration

Admin Tip: QoS

All handsets operating on a given AP radio must have the same QoS setting. All APs supporting the handsets must be configured to enable the corresponding features.

1. Power-on and connect the APs to the network. Wait a few minutes for the APs to find the controller.
2. Verify the APs are associated to the WLC.
3. From the main menu, click **Monitor**.



Configuration for handsets running in 802.11b, b/g mixed mode, g only mode in 8020/8030 handsets or 2.4 GHz in 84-Series handsets

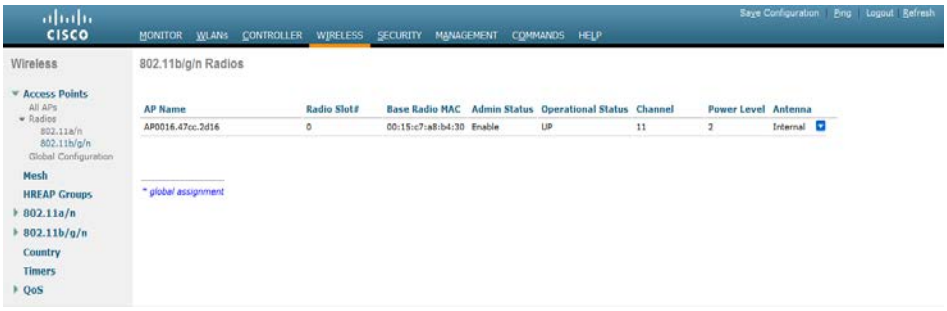
Admin Tip: When to use g-only

When 8020/8030 handsets are set to g only mode, they support the higher g data rates. In g only mode, however, the handset will not detect 802.11b clients and will not provide protection. G only mode in these handsets should be used only if there is no possibility of an 802.11b client or the network will experience data corruption.

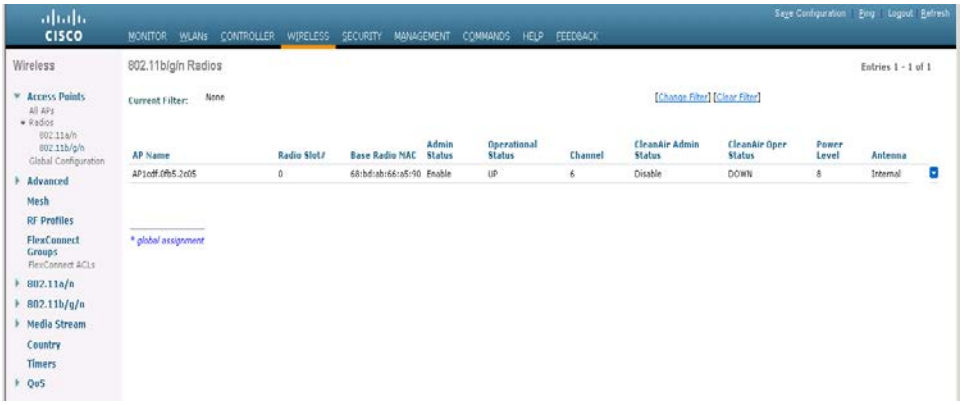
1 From the main menu, click **Wireless**.

2 In the navigation pane, under Access Points click **Radios**, then select **802.11b/g/n**. All the APs that are connected should be listed, showing their Operational Status as **UP**.

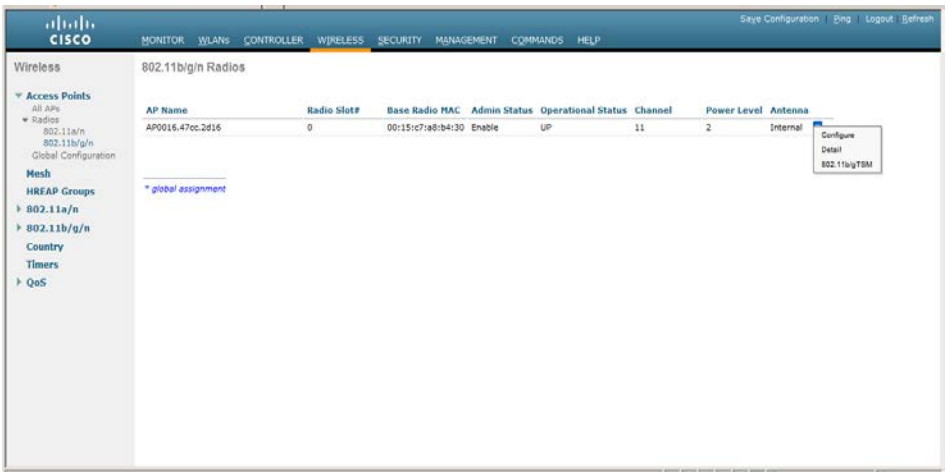
Cisco 6.0 Version



Other Versions (for example)



3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:



Settings: Power and channel settings

Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested.

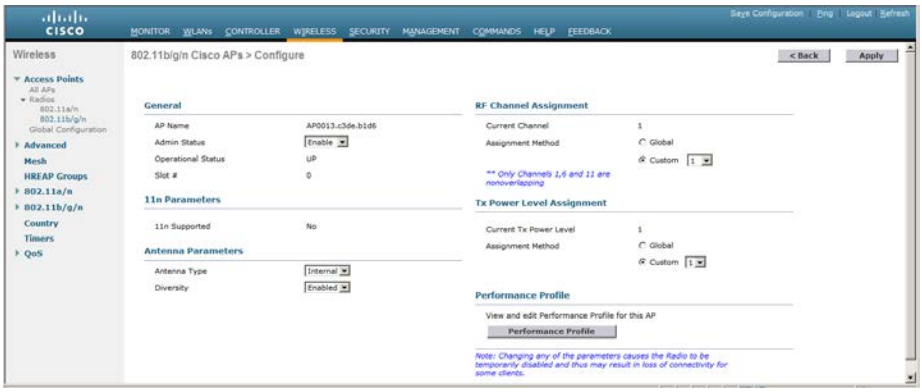
For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using only channels **1**, **6** and **11**.

a Set Admin Status to **Enable**.

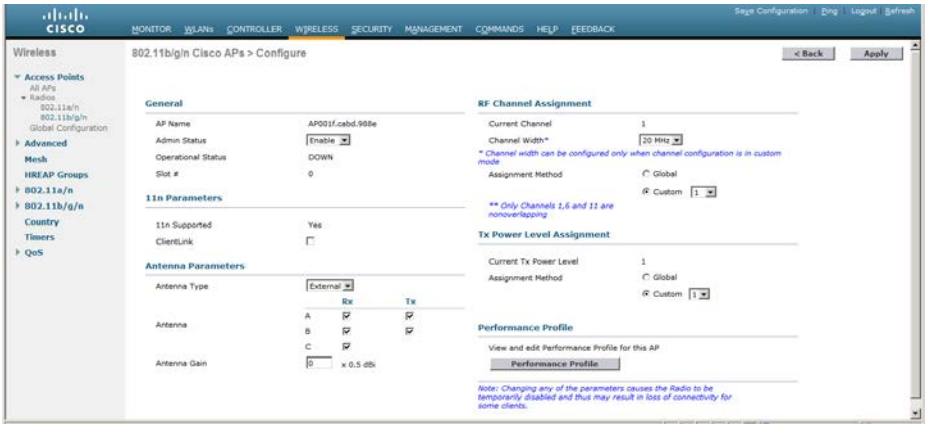
b Configure any other settings that might be relevant to your deployment as needed.

c Click the **Apply** button to save all changes.

Screenshot for access points with internal antennas:



Screenshot for sample access point with three external antennas:



4 In the navigation pane under 802.11b/g/n, click **Network**. Set network parameters as follows:

a Set 802.11b/g Network Status to **Disable**. The radio will be re-enabled after setting radio parameters.

Admin Tip: Data Rates

For setting up the **Data Rates,** please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

802.11 Radio Standard	*Minimum Available Signal Strength (RSSI)*	*Maximum "Mandatory" Data Rate*
802.11b	-75 dBm	1 Mb/s
	-65 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

Web Info: RF Deployment reference

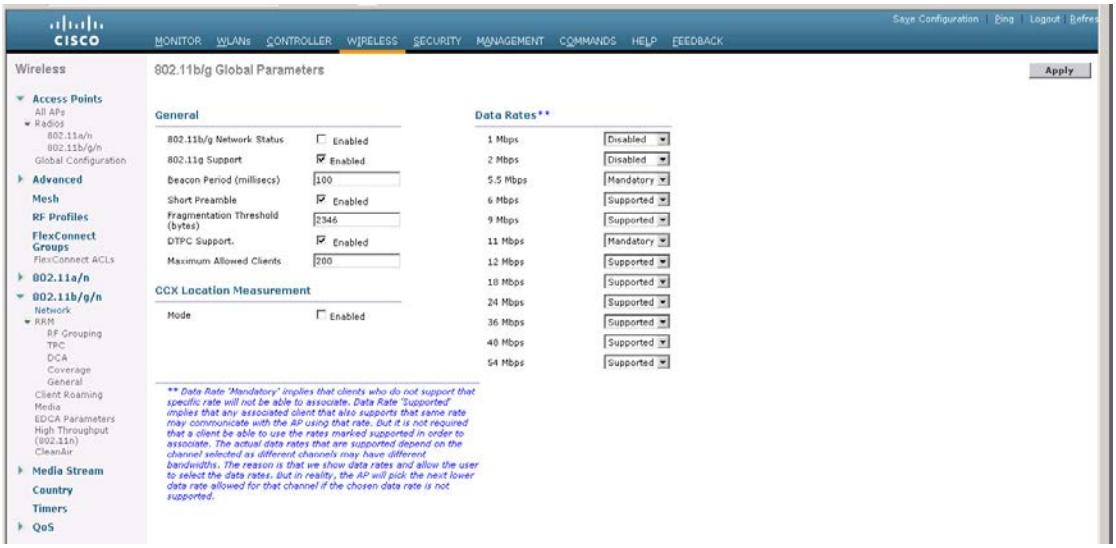
For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide to Network Design Considerations for Spectralink Wireless Telephone*.

b Use the default **Fragmentation Threshold** (2346 bytes).

c Set the **Beacon Period** to **100**.

d Set the 1 Mbps and 2 Mbps settings to **Disabled**.

e Click the **Apply** button to save the settings.



Admin Tip: Enable Admission Control

Admission Control (ACM) must be enabled on both the Voice and Video AC when the handset is configured for Admission Control Mandatory.

5 For Cisco 6.0, in the navigation pane under 802.11b/g/n, select **Voice**.
For Cisco 7.0 and later, in the navigation pane under 802.11 b/g/n, select Media, then select the **Voice** tab.

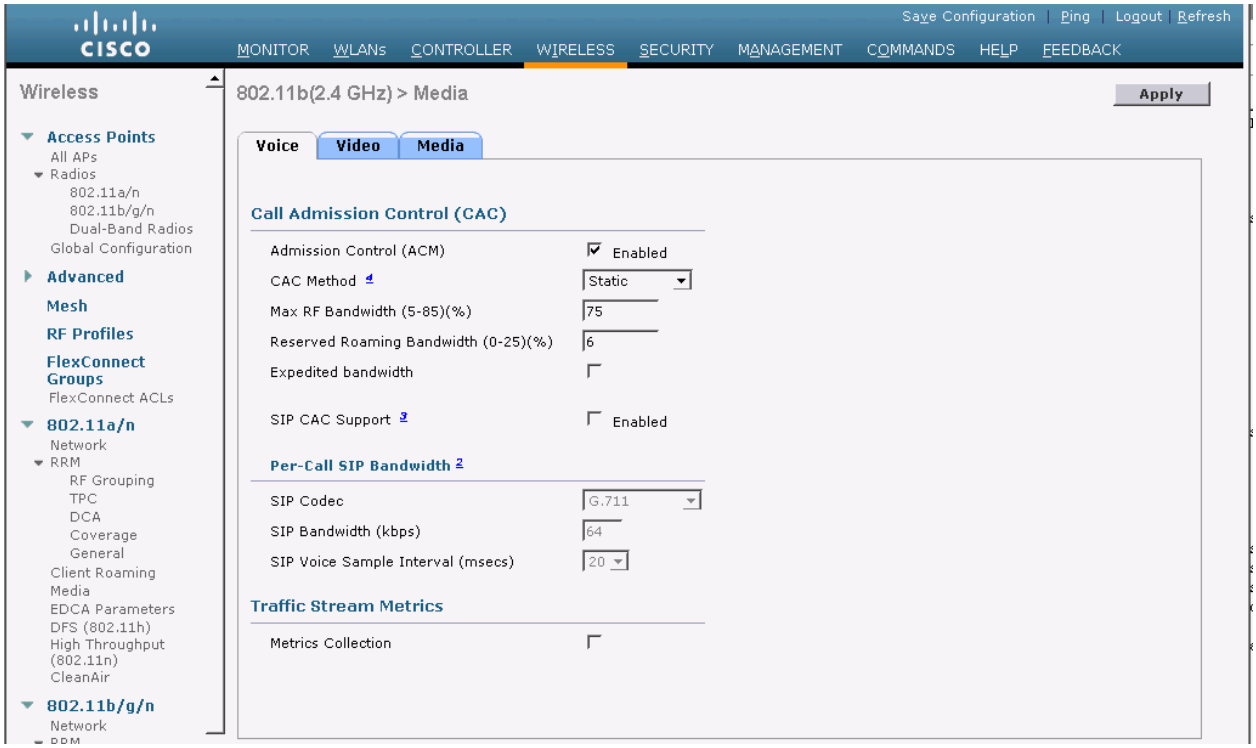
6 Select the **Admission Control (ACM)** checkbox. If CAC Method is available, select **Static** from the drop down list. Set the Max RF Bandwidth to **45** for 8020/8030 handsets or **50** for 84-Series handsets to limit the bandwidth allocated to handsets to a value tested to provide good performance. (If both handset types are present, use 50.) If available, ensure that the Reserved Roaming Bandwidth is set to 6%.

Admin Tip: Use the Static CAC Method.

It is very important to choose the Static CAC method to avoid limiting calls when there is heavy background traffic.

Admin Tip: Disable WLAN before changing Admission Control settings.

Any WLAN using the network must be disabled before changing Admission Control settings.

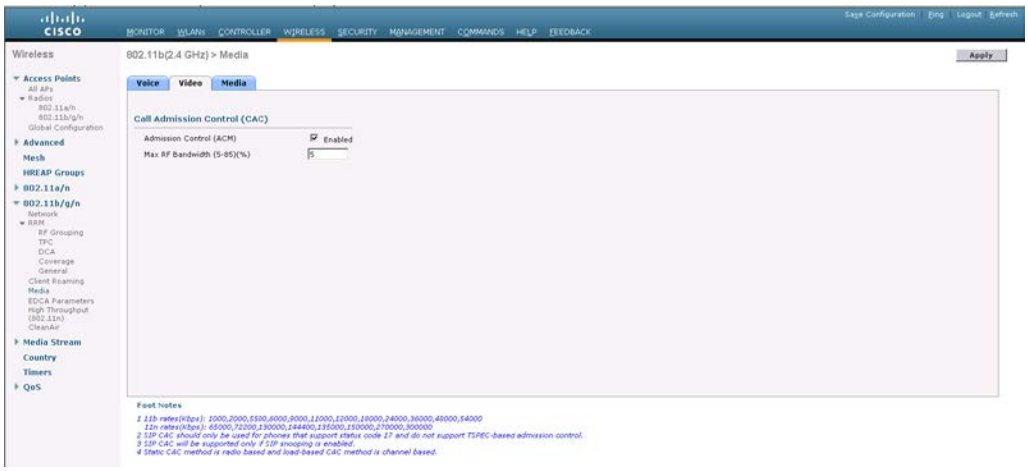


7 For Cisco 6.0, in the navigation pane under 802.11b/g/n, select **Video**. For Cisco 7.0 and later versions, in the navigation pane under 802.11b/g/n, select **Media**, then select the **Video** tab.

8 Select the **Admission Control (ACM)** checkbox. Set the Max RF Bandwidth for Video to **5**. If available, ensure that the Reserved Roaming Bandwidth is set to 5%.

Admin Tip: Disable WLAN before changing Admission Control settings.

Any WLAN using the network must be disabled before changing Admission Control settings.



9 Click the Apply button to save the settings.

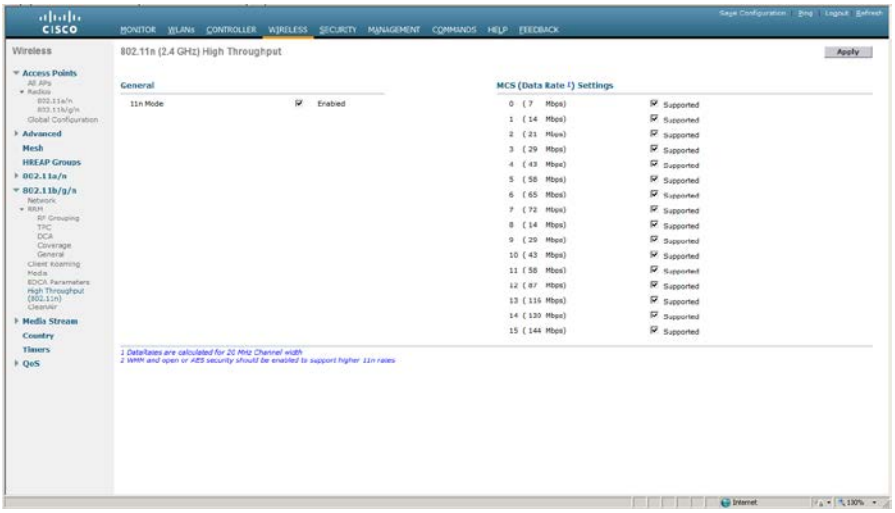
10 In the navigation pane under 802.11b/g/n, select **Network**.

11 Enable 802.11b/g Network Status and 802.11g Support if Spectralink Wireless Telephones are configured for 802.11b & b/g mixed or g only mode in 8020/8030 handsets or 2.4 GHz in 84-Series handsets.

12 Click the **Apply** button to save the settings.

Configuring 802.11n

1 In the navigation pane under 802.11 b/g/n, select **High Throughput** (802.11n). Check the radio box to enable **11n** mode and allow all data rates to be supported.



2 **Disable** msdu aggregation:

a Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.

b Enter the commands:

```
config 802.11b 11nsupport a-msdu tx priority all disable
save config
```

3 If an 1142 ap is in use, disable mpdu aggregation.

a Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.

b Enter the commands:

```
config 802.11b 11nsupport a-mpdu tx priority all disable
save config
```

4 Click the **Apply** button to save the settings.

5 In the navigation pane under 802.11b/g/n, select **Network**.

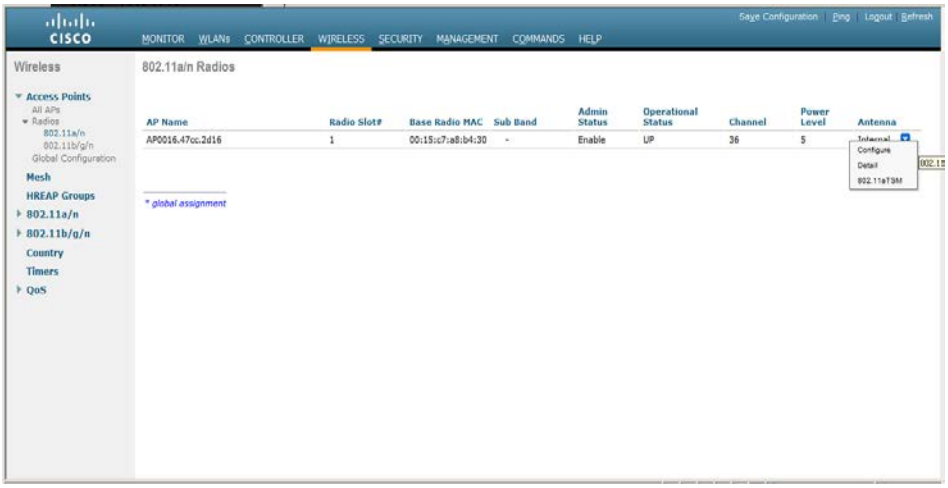
6 For 802.11b/g Network Status, click the **Enabled** check box.

Configuration for handsets running in 802.11a mode in the 8020/8030 handsets and using the 5 GHz radio in the 84-Series handsets

1 From the main menu, click **Wireless**.

2 In the navigation pane, under Access Points click **Radios**, then select **802.11a /n**. All the APs that are connected should be listed, showing their Operational Status as **UP**.

3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:



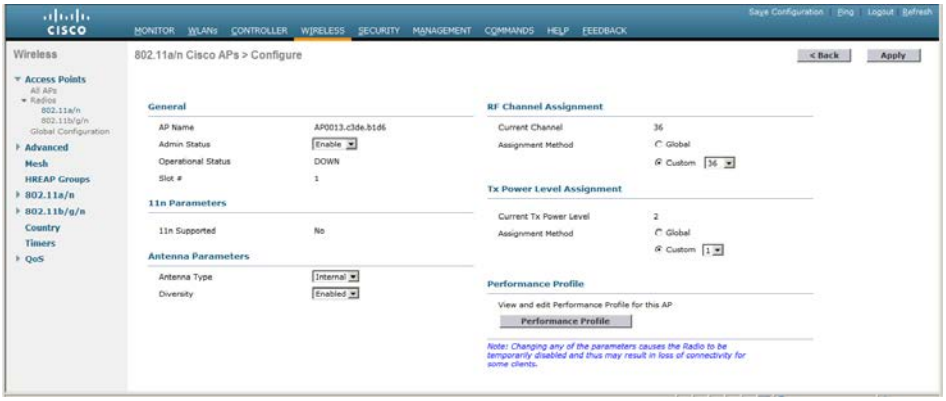
Settings: Power and channel settings

Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested. For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using non-overlapping channels.

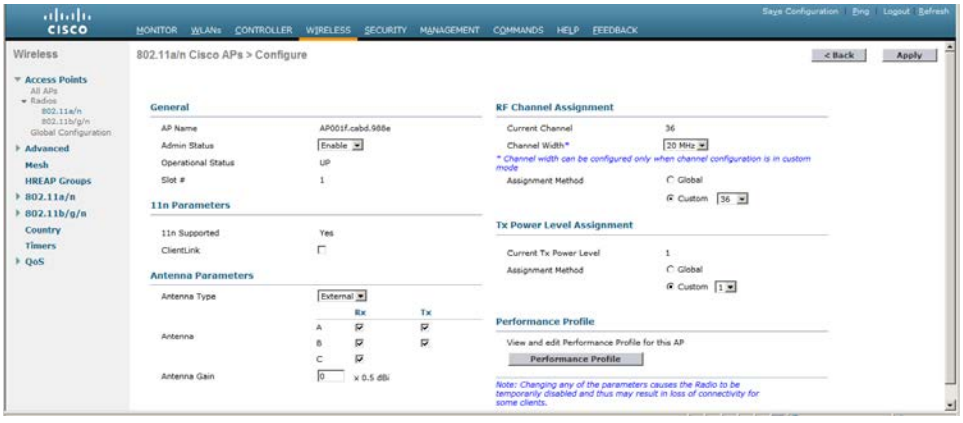
a Configure any other settings that might be relevant to your deployment as needed. In version 7.0.220.0, select only one antenna for transmission when using 80xx handsets. The CSD (cyclic shift diversity) algorithm has an incompatibility, which is not present in the other releases.

b Click the **Apply** button to save all changes.

Screenshot for access points with internal antennas:



Screenshot for access points with external antennas:



4 In the navigation pane under 802.11a/n, click **Network**. Set the network parameters as follows:

a Set **802**.11a **Network Status** to **Disable**; the radio will be re-enabled after setting radio parameters

b For setting up the **Data Rates,** please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. The handset requires the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

802.11 Radio Standard	*Minimum Available Signal Strength (RSSI)*	*Maximum "Mandatory" Data Rate*
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

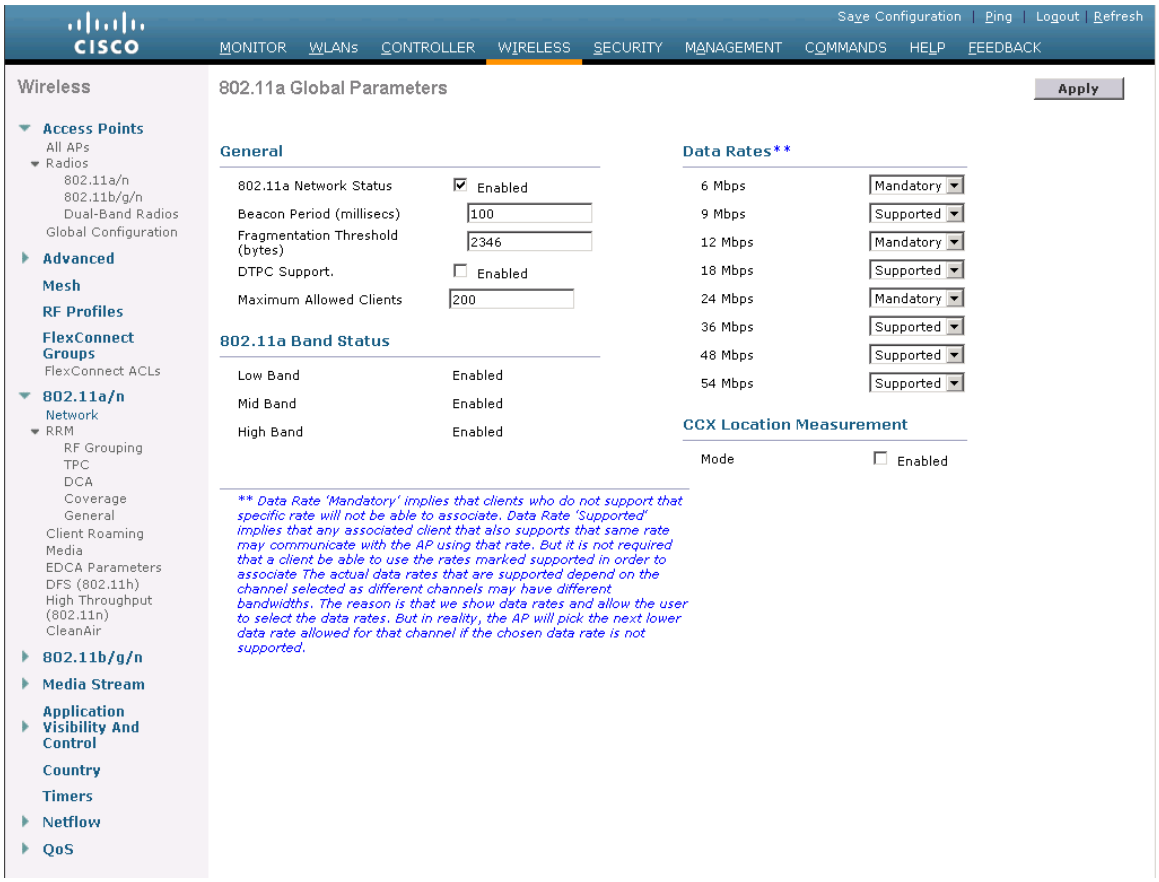
Web Info: RF Deployment Information

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide to Network Design Considerations for Spectralink Wireless Telephone*.

c Use the default **Fragmentation Threshold** (2346 bytes).

d Set the **Beacon Period** to **100**.

e Click the **Apply** button to save the settings.



5 If DFS channels are used in the deployed network, in the navigation pane under 802.11a/n, select DFS (802.11h). Check the Channel Announcement radio box to cause the AP to advertise Spectrum Management. If the AP does not advertise Spectrum Management, Spectralink handsets will not connect on DFS channels (bandwidth shared with radar facilities).

Admin Tip: Admission Control

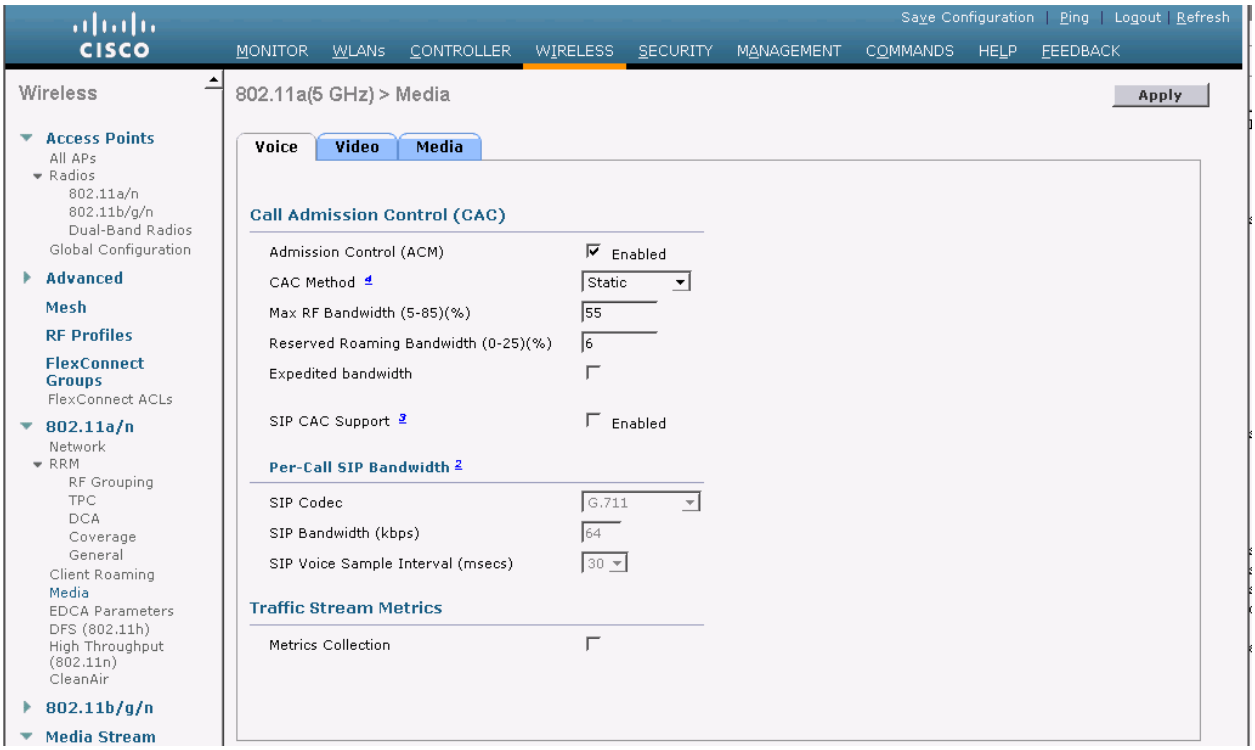
Admission Control (ACM) must be enabled on both the Voice and Video AC when the handset is configured for Admission Control Mandatory.

6 For Cisco 6.0, in the navigation pane under 802.11a/n, select **Voice**.
For Cisco 7.0 and later versions, in the navigation pane underneath 802.11 a/n, select **Media**, then select the **Voice** tab.

7 Select the **Admission Control (ACM)** checkbox. If **CAC Method** is available, select **Static** from the drop down list. Set the Max RF Bandwidth to **35** for 8020/8030 handsets or **55** for 84-Series handsets to limit the bandwidth allocated to handsets to a value tested to provide good performance. (If both handset types are present, use **45**.) If available, ensure that the Reserved Roaming Bandwidth is set to 6%.

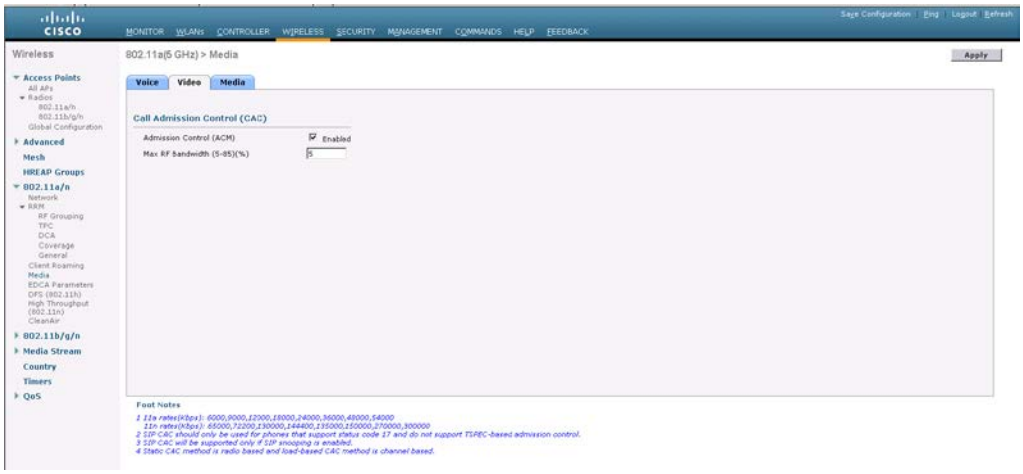
Admin Tip: Use the Static CAC Method.

It is very important to choose the Static CAC method to avoid limiting calls when there is heavy background traffic.



8 For Cisco 6.0, in the navigation pane under 802.11a/n, select **Video**.
For Cisco 7.0 and later versions, in the navigation pane under 802.11a/n or 802.11a/n/ac, select Media, then select the **Video** tab. Set the Max RF Bandwidth for Video to **5**. If available, ensure that the Reserved Roaming Bandwidth is set to 5%.

9 Select the **Admission Control** (**ACM**) checkbox.



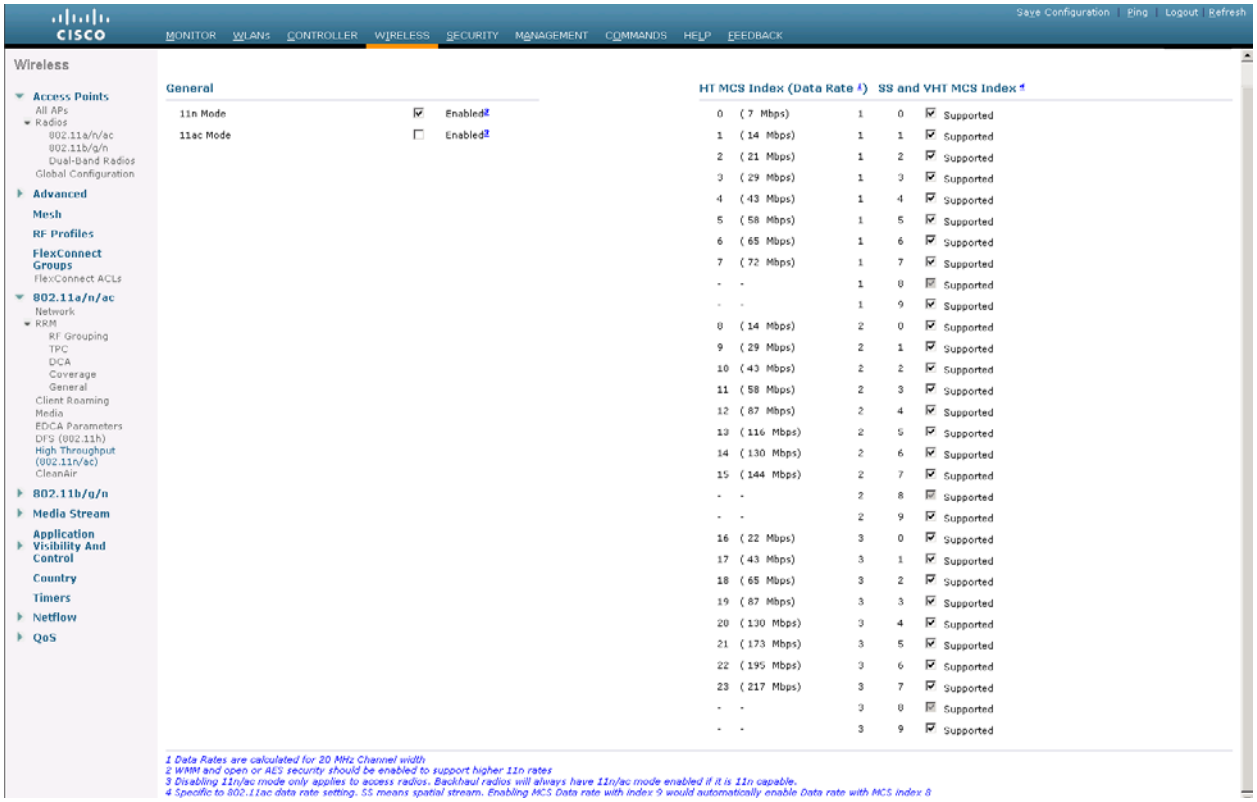
10 Click the **Apply** button to save the settings.

Configuring 802.11n:

1 In the navigation pane under 802.11 a/n, select **High Throughput** (**802.11n**). Check the radio box to enable 11n mode and allow all data rates to be supported.

802.11a/n AP's

802.11a/n/ac AP's



Admin Tip: 802.11ac

Spectralink has not yet been tested with 802.11ac clients in the network. It is known that the handsets operate properly with 802.11ac turned off as shown.

2 **Disable** msdu aggregation:

a Connect to the CLI as described in the section "Configuring a New Controller Starting from Factory Defaults".

b Enter the commands:

```
config 802.11a 11nsupport a-msdu tx priority all disable
save config
```

3 If an 1142 ap is in use, disable mpdu aggregation.

a Connect to the CLI as described in the section "Configuring a New Controller Starting from Factory Defaults".

b Enter the commands:

```
config 802.11a 11nsupport a-mpdu tx priority all disable
save config
```

4. In the navigation pane under 802.11a/n, select **Network**.
5. For 802.11a Network Status, click the **Enabled** check box.
6. Click the **Apply** button to save the settings.

Setting up the SSID

Voice and data must be on separate SSIDs to prioritize voice traffic. The voice SSID must be set to **Platinum** for **Quality of Service** and the data SSID must be set to **Silver** for **Quality of Service**.

1. From the main menu, click **WLANs**.
2. In the WLANs screen, select **Create New** from the drop down list and click **Go**.

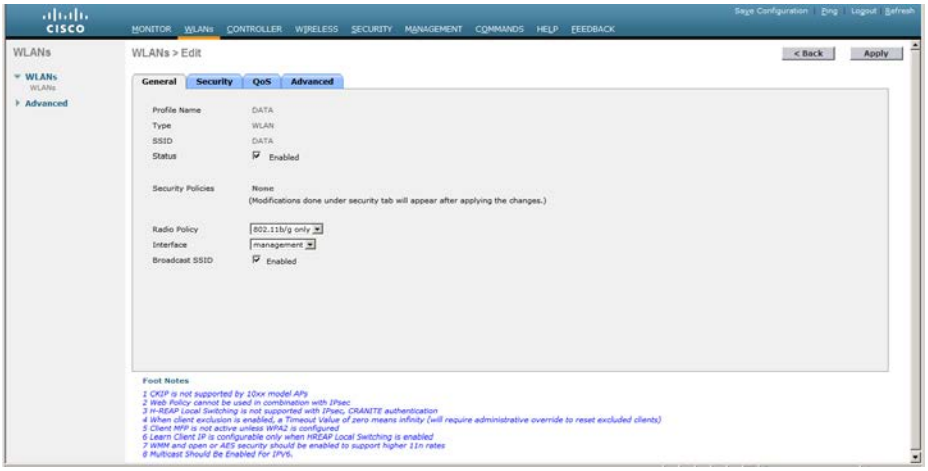
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
WLANs
Advanced
Entries 0 - 0 of 0
Current Filter: None [Change Filter] [Clear Filter]
Create New
Go
WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

3. Enter the Profile Name and SSID.
4. Click the **Apply** button twice.

Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
WLANs
Advanced
Entries 1 - 2 of 2
Current Filter: None [Change Filter] [Clear Filter]
Create New
Go
WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies
1 WLAN Voice 101V Disabled [WPA2][Auth(802.1X)]
2 WLAN Data 101D Disabled [WPA2][Auth(802.1X)]

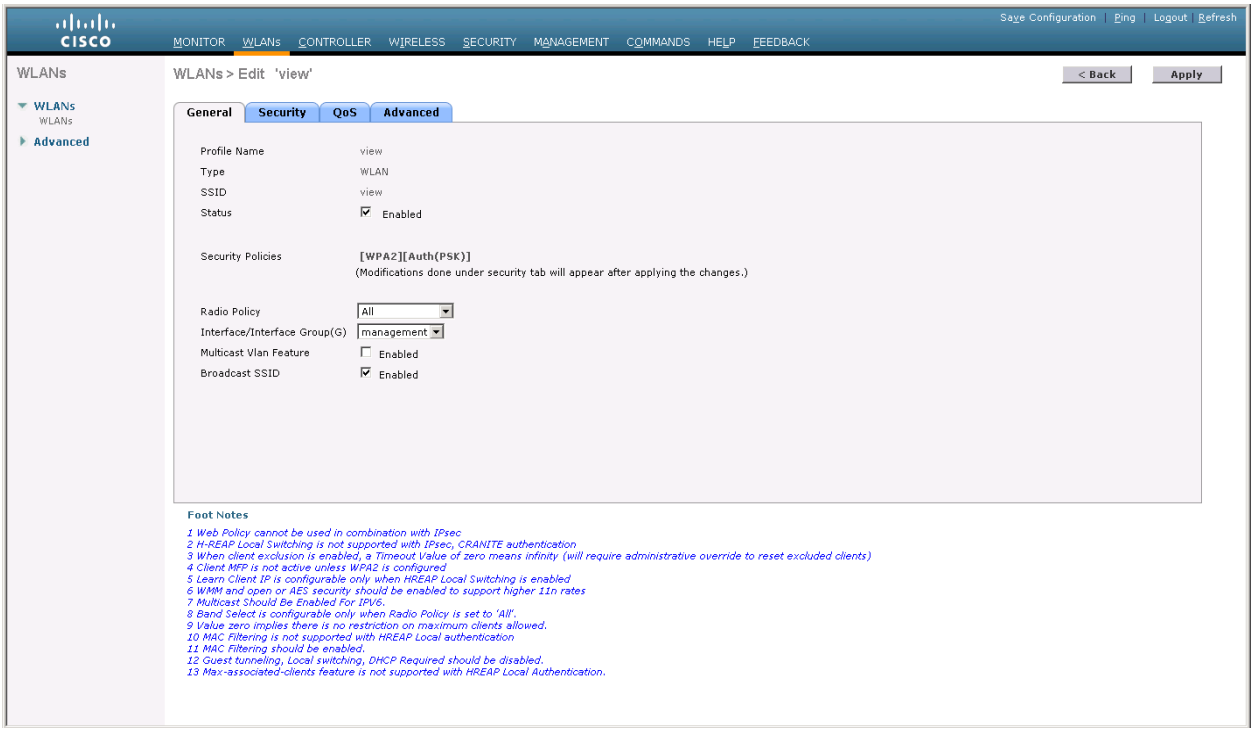
5. Select the Profile Name for the voice SSID.
6. Under the General tab, verify the Radio Policy corresponds to the Spectralink Wireless Telephone configuration.
   - When Radio Policy is configured for 802.11b/g only, the handsets should be configured for 802.11b & b/g mixed in 8020/8030 handsets and 2.4 GHz in 84-Series handsets.
   - When Radio Policy is configured for 802.11a only, the handsets should be configured for 802.11a in 8020/8030 handsets and 5 GHz in 84-Series handsets.
   - When Radio Policy is configured for 802.11g only, the handsets should be configured for 802.11g only in 8020/8030 handsets and 2.4 GHz in 84-Series handsets.
   - When Radio Policy is configured for All, the handsets may be configured to any of the settings required.
7. For Status, select the **Enabled** check box.

Cisco 6.0 Versions:



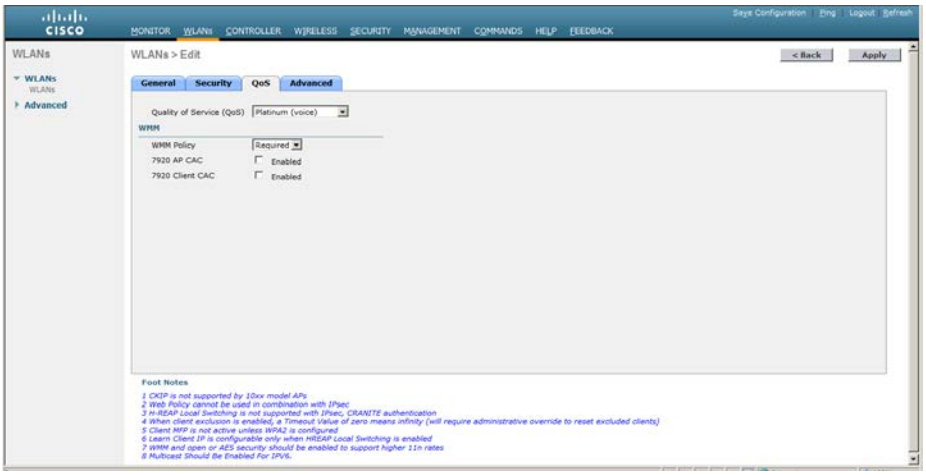
Other versions:

(Ensure that the Multicast Vlan Feature remains unchecked for proper PTT performance.)


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'view'
< Back
Apply
General
Security
QoS
Advanced
Profile Name
view
Type
WLAN
SSID
view
Status
Enabled
Security Policies
[WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G)
management
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
Foot Notes
1 Web Policy cannot be used in combination with IPsec
2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when HREAP Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Multicast Should Be Enabled For IPV6.
8 Band Select is configurable only when Radio Policy is set to 'All'.
9 Value zero implies there is no restriction on maximum clients allowed.
10 MAC Filtering is not supported with HREAP Local authentication
11 MAC Filtering should be enabled.
12 Guest tunneling, Local switching, DHCP Required should be disabled.
13 Max-associated-clients feature is not supported with HREAP Local Authentication.

8 Under the QoS tab, set Quality of Service to **Platinum**. This is the required setting for voice traffic.

9 Set WMM Policy to **Required**.

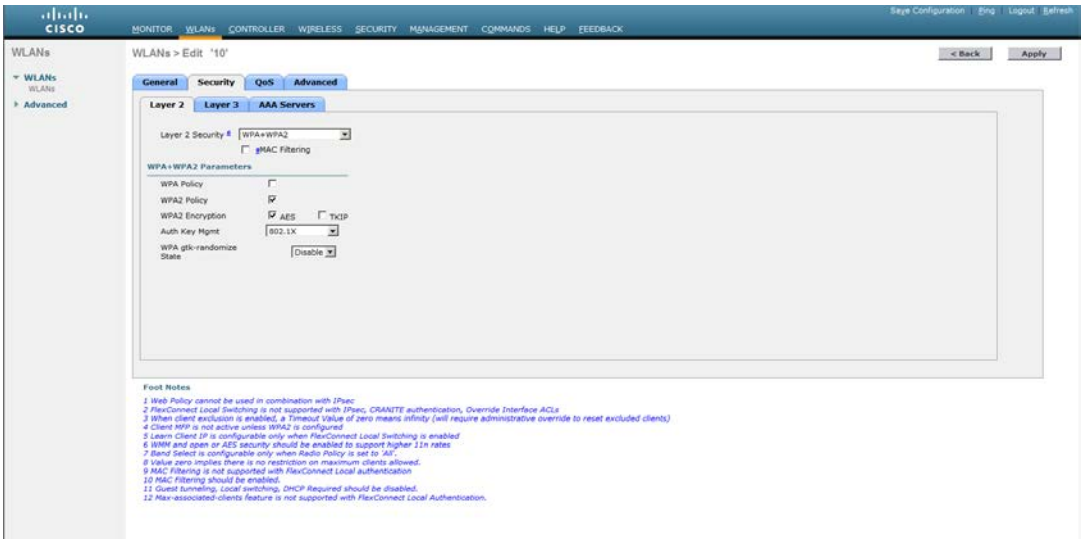


10 Under the Security tab, at Layer 2 Security select the desired security policy from the drop-down list.

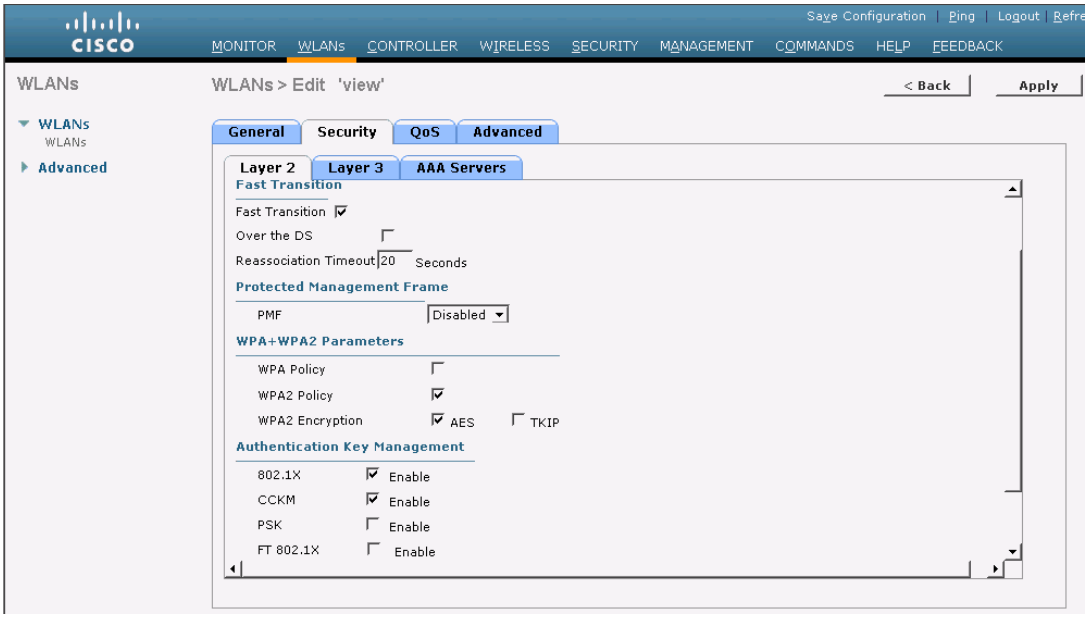
- For WPA2-PSK, under WPA+WPA2 Parameters:
  - **i** Select the **WPA2-Policy** check box.
  - **ii** Select the **AES** check box for **WPA2-Encryption**.
  - **iii** At **Auth Key Mgmt** select **PSK** from the drop-down list.
  - **iv** If present (7.2. and later versions), ensure that **WPA gtk-randomize State** is set to **Disable**. The Fast Transition and FT PSK radio boxes may be checked or unchecked as desired.
- For WPA-PSK, under WPA+WPA2 Parameters:
  - **i** Select the WPA-Policy check box.
  - **ii** Select the TKIP check box for WPA Encryption.
  - **iii** At Auth Key Mgmt select PSK from the drop-down list. The PSK Format may be selected as ASCII or HEX for both WPA-PSK and WPA2-PSK policies.
  - **iv** If present (7.2 and later versions), ensure that the Fast Transition and FT boxes remain unchecked.
  - **v** If present (7.2. and later versions), ensure that WPA gtk-randomize State is set to Disable. The Fast Transition and FT PSK radio boxes may be checked or unchecked as desired.
- For WPA2-Enterprise (802.1X), select WPA+WPA2 Parameters:
  - **i** Select the **WPA2 Policy** check box.
  - **ii** Select the **AES** check box for **WPA2 Encryption**.
  - **iii** At **Auth Key Mgmt**, select **802.1X+CCKM** from the drop-down list.
  - **iv** If present (7.2. and later versions), ensure that **WPA gtk-randomize State** is set to **Disable**.

- **v** If present (7.2 and later versions), the **Fast Transition** radio box may be checked to permit other devices to use 802.11r but the **FT 802.1x** radio box must not be checked as it limits network access to 802.11r devices only.

Cisco 6.0 and 7.0 Versions:



Cisco 7.2 and later Versions:



11 Under the Advanced tab

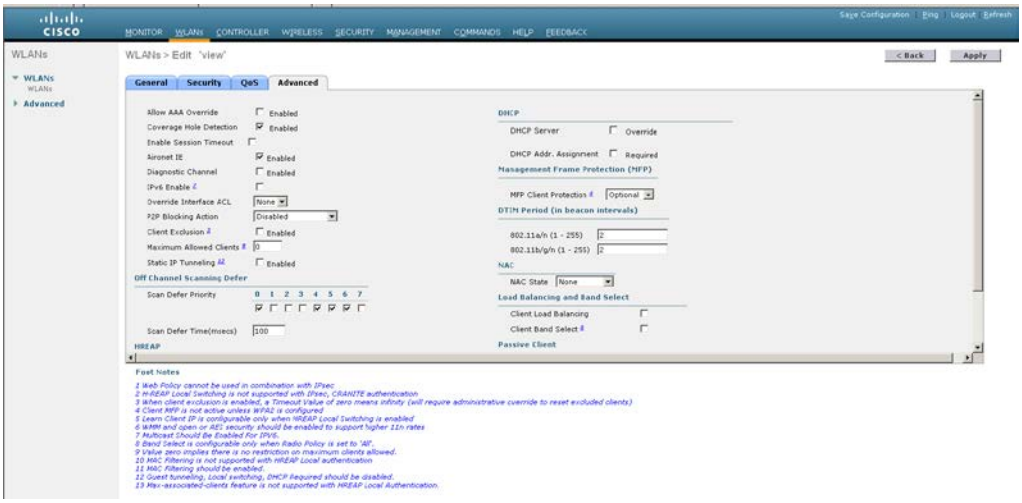
- **a** Set the DTIM to **2** for the radio that corresponds to the Spectralink Wireless handset configuration.

b Ensure the Enable Session Timeout box is unchecked and that Client Exclusion is disabled.

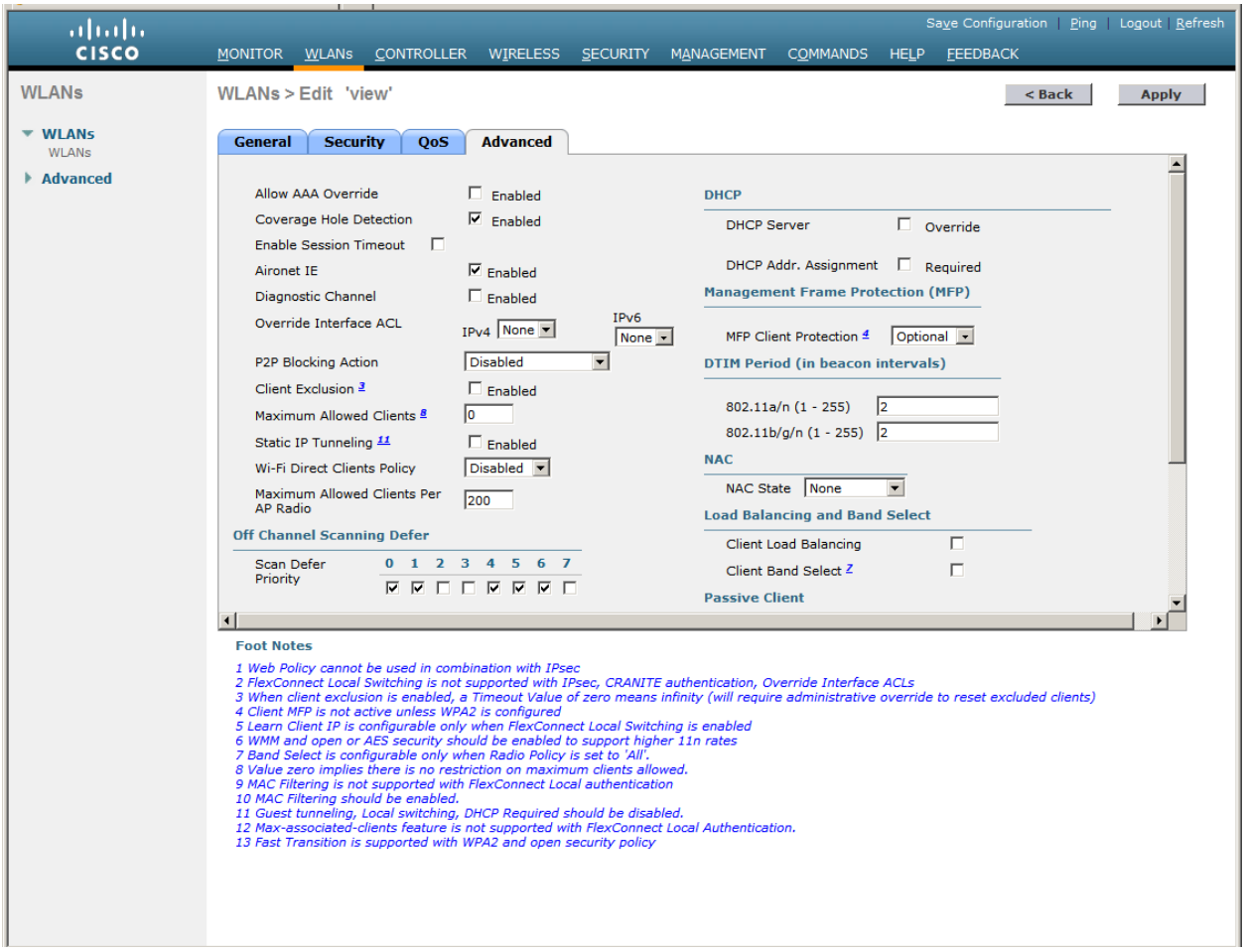
c Uncheck the Client Load Balancing and Client Band Select boxes.

d Check off-channel scanning defer for the 0 priority class (prevents contention between off-channel scanning and PTT).

Cisco 6.0 and 7.0 versions:



Cisco 7.2 and later versions:


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'view'
< Back
Apply
General
Security
QoS
Advanced
Allow AAA Override
Enabled
Coverage Hole Detection
Enabled
Enable Session Timeout
Aironet IE
Enabled
Diagnostic Channel
Enabled
Override Interface ACL
IPv4 None
IPv6 None
P2P Blocking Action
Disabled
Client Exclusion 3
Enabled
Maximum Allowed Clients 8
0
Static IP Tunneling 11
Enabled
Wi-Fi Direct Clients Policy
Disabled
Maximum Allowed Clients Per AP Radio
200
Off Channel Scanning Defer
Scan Defer Priority
0 1 2 3 4 5 6 7
DHCP
DHCP Server
Override
DHCP Addr. Assignment
Required
Management Frame Protection (MFP)
MFP Client Protection 4
Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255)
2
802.11b/g/n (1 - 255)
2
NAC
NAC State
None
Load Balancing and Band Select
Client Load Balancing
Client Band Select 7
Passive Client
Foot Notes
1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.
13 Fast Transition is supported with WPA2 and open security policy

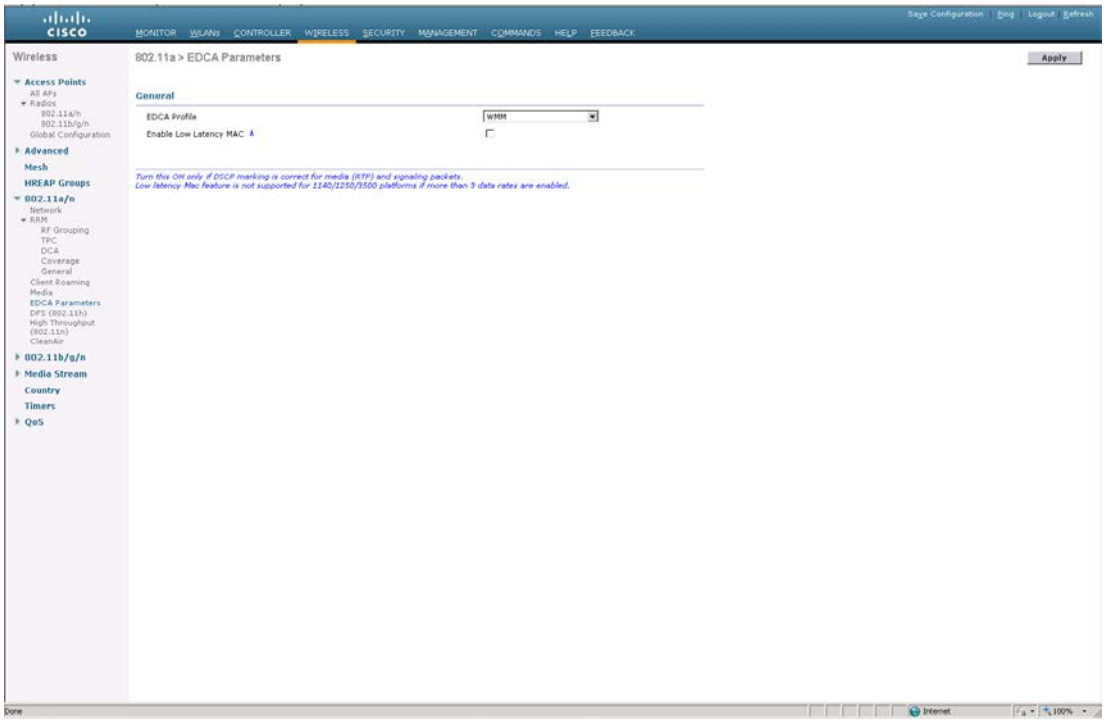
12 Click the **Apply** button to save all changes.

Setting up the EDCA parameters profile

The EDCA parameters must be set to the WMM setting after the WLAN network QoS has been set.

Configuration for handsets running in 802.11a mode mode in 8020/8030 handsets or 5 GHz in 84-Series handsets

1. In the navigation pane under 802.11a/n, select **EDCA Parameters**.
2. Ensure that **WMM** is selected from the drop-down list.
3. Click **Apply**.



Configuration for handsets running in 802.11b/g mode, 802.11b and b/g mixed mode, or 802.11 g only mode in 8020/8030 handsets or 2.4 GHz in 84-Series handsets

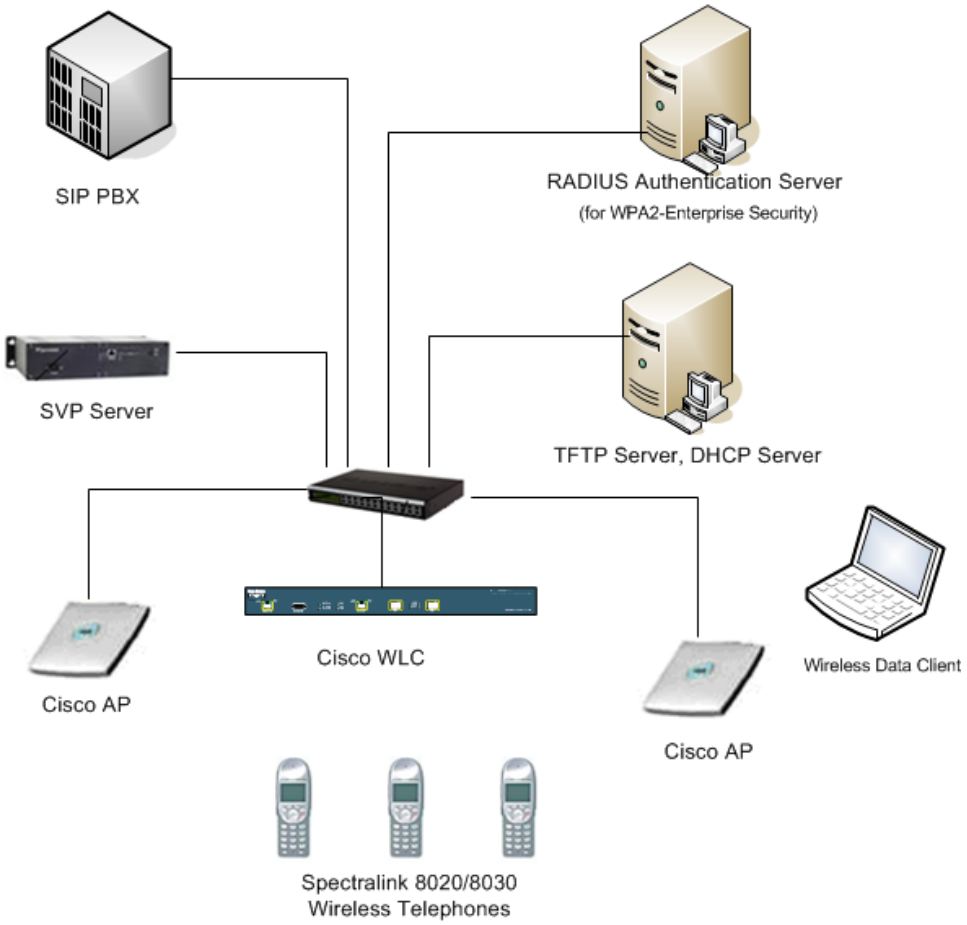
1. In the navigation pane under 802.11b/g/n, select **EDCA Parameters**.
2. Ensure that **WMM** is selected from the drop-down list.
3. Click **Apply**.

Chapter 2: Configuration for SVP Operation

Introduction

Spectralink 8020/8030 handsets can be configured for SVP QoS from the WLAN Settings menu using the Custom selection. Spectralink 84-Series handsets do not support SVP.

Network Topology



Note: Example only

This configuration is not applicable to all customer environments.

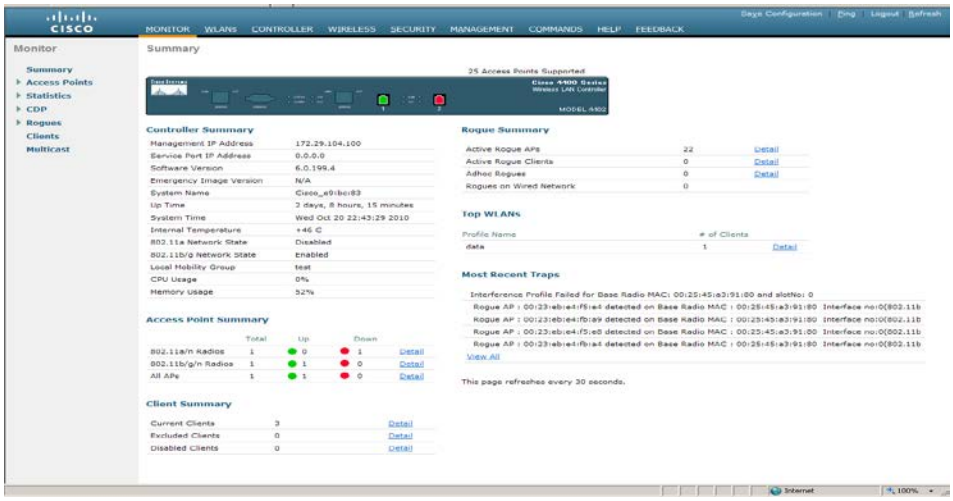
Configuring a New Controller Starting from Factory Defaults

Initial provisioning of the controller is done via the command line interface (CLI).

1. Connect a null modem serial cable between the console port of the controller and the serial port of a PC.
2. Open a terminal program, such as Hyper Terminal, and configure the port settings to 9600 baud, no parity, 8 data bits and 1 stop bit.
3. Power-on the controller. Status of the controller's boot process will appear as the controller is powering up. Once the controller is running, it will prompt you to run the Startup Wizard.
4. The Startup Wizard provides for an easy means to perform initial controller setup and provisioning. Refer to the Installation and Startup Guide for the Cisco 5500 Series WLC, or other appropriate controller, found at Cisco's website. This document contains a detailed explanation of using the Startup Wizard for the 5500: http://www.cisco.com/en/US/docs/wireless/controller/5500/install/guide/ctrl5500.html. Once the controller has been configured via the Startup Wizard, the remaining configuration can be configured through the switch-web interface using a Web browser (Cisco recommends using MS IE 6.0+).
5. If necessary, the controller can be reset to factory defaults. To reset the WLC to factory default, you must reboot, then type Recover-config at the CLI. This only works before the first time a user logs in via the console.

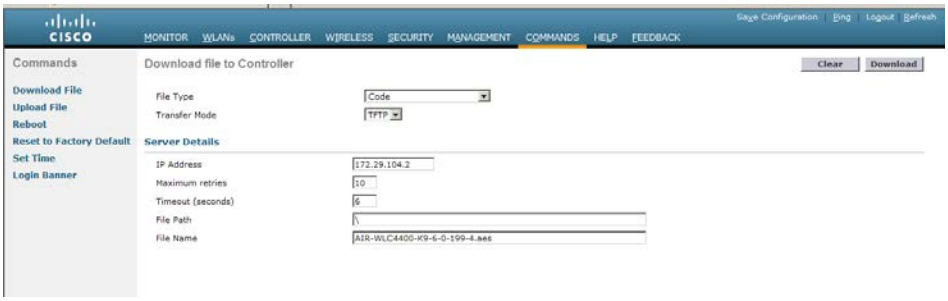
Connecting to the Controller via a Browser

1. Connect to the WLC by pointing your internet browser to the URL: https<IP_Addr> (where <IP_Addr> is the IP address of the management interface of the WLC).
2. Click the **Login** prompt. The default User Name and Password is admin.
3. Once logged in properly, a page similar to the one below displays.



Installing Software

1. To check the installed version of software, listed in the Product Summary, click Monitor from the main menu.
2. In the navigation pane, click Summary. The heading labeled Software Version shows the current software version.
3. Download the appropriate software for your model of controller from the Cisco website.
4. Set up a Trivial File Transfer Protocol (TFTP) server running on a PC to download the file to the controller.
5. From the main menu, click **Commands**.
6. In the navigation pane, click **Download File**.
7. Fill in the download parameters:
   a. For **File Type**, select **Code**.
   b. For **TFTP Server**, type in the IP Address of the TFTP server.
   c. Add the **File Path** (this is the path in the TFTP server's root directory and not the system path where the TFTP server is located) and **File Name** of the firmware file to download.
   (Note the example simply uses the /designator for the root TFTP directory.) Point the TFTP server to the code.
8. Click **Download** and allow a few minutes for the download to complete.



9. Reboot the Controller.

Controller Setup

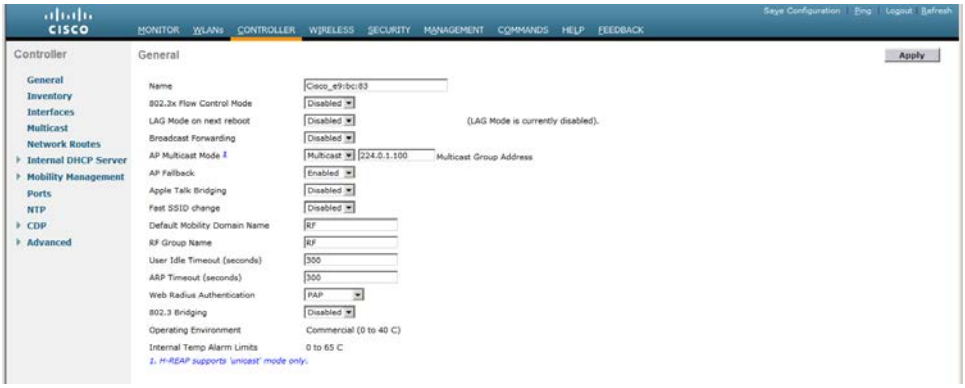
The initial setup of the controller is shown below.

Admin Tip: Example configuration

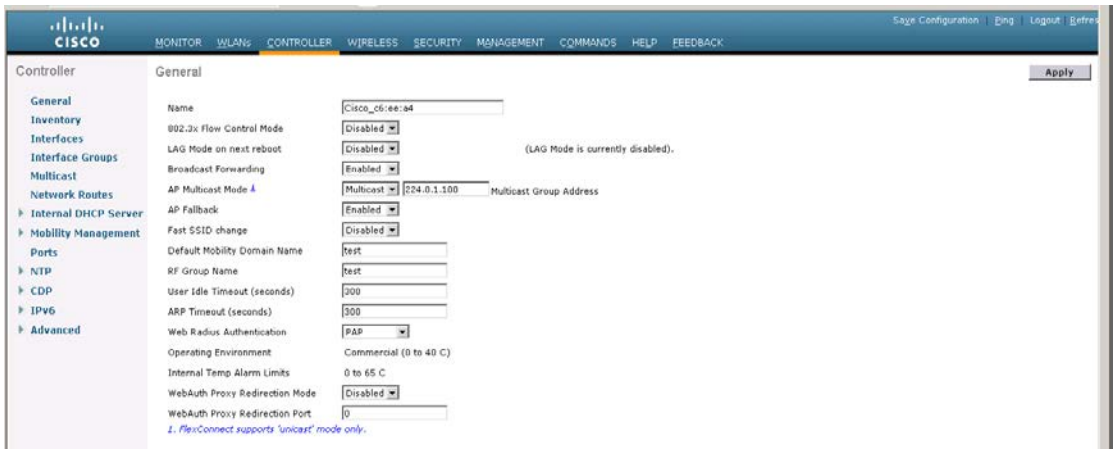
The setup instructions outlined in this document are for the configuration shown in the diagram only. Your configuration may differ, and the appropriate adjustments must be made.

1. From the main menu, click **Controller**.
2. Set the AP Multicast Mode to Multicast and enter a multicast IP address that is currently not being used on your network for the Multicast Group Address.
3. Click the **Apply** button.

Cisco 6.0 versions:



Cisco 7.0 and 7.2 versions:



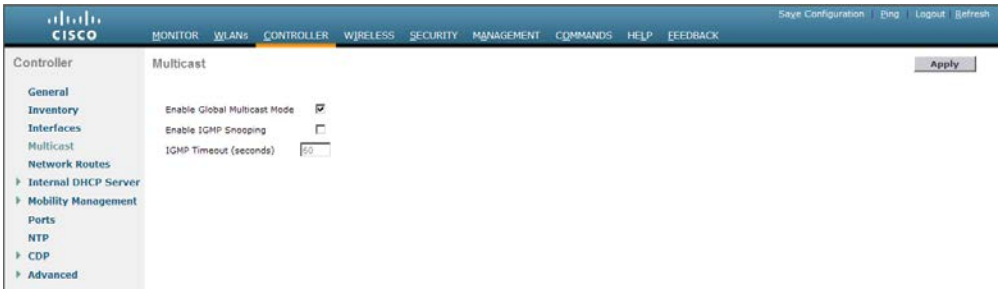
Cisco 7.3 and later versions:

4 Click **Multicast** from the options on the left side of the screen.

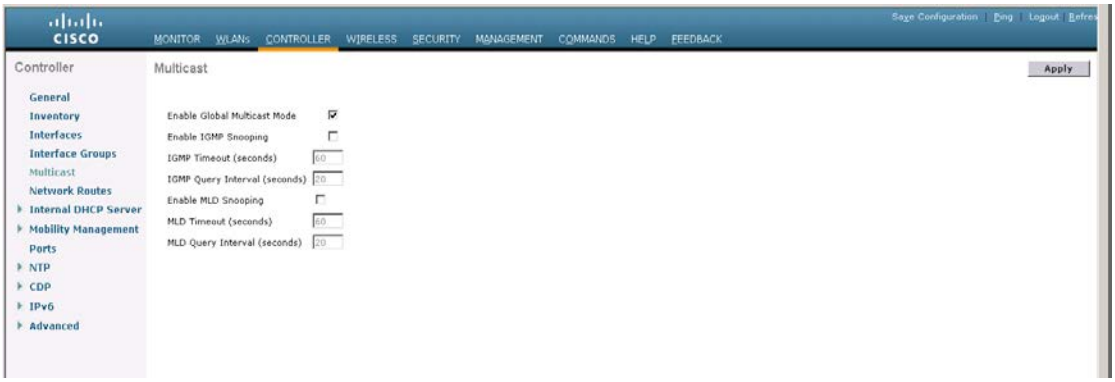
5 Select **Enable Global Multicast Mode** checkbox.

6 Click the **Apply** button.

Cisco 6.0 versions:



Cisco 7.0 and 7.2 versions:



Cisco 7.3 and later versions:

7 Click **Save Configuration**.

Connecting APs

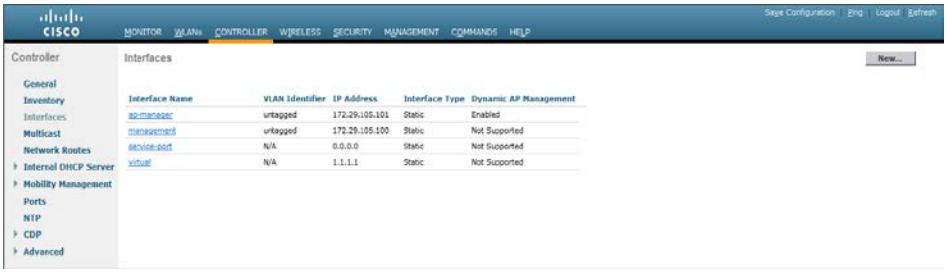
As the APs are connected to the network, they should automatically find the controller via the CAPWAP discovery algorithms. The Dynamic Host Configuration Protocol (DHCP) server will assign each AP an IP address.

Admin Tip: DHCP server

You can configure a DHCP server to run on a remote PC for a small deployment. However, for large-scale deployments, an enterprise-grade DHCP server must be used.

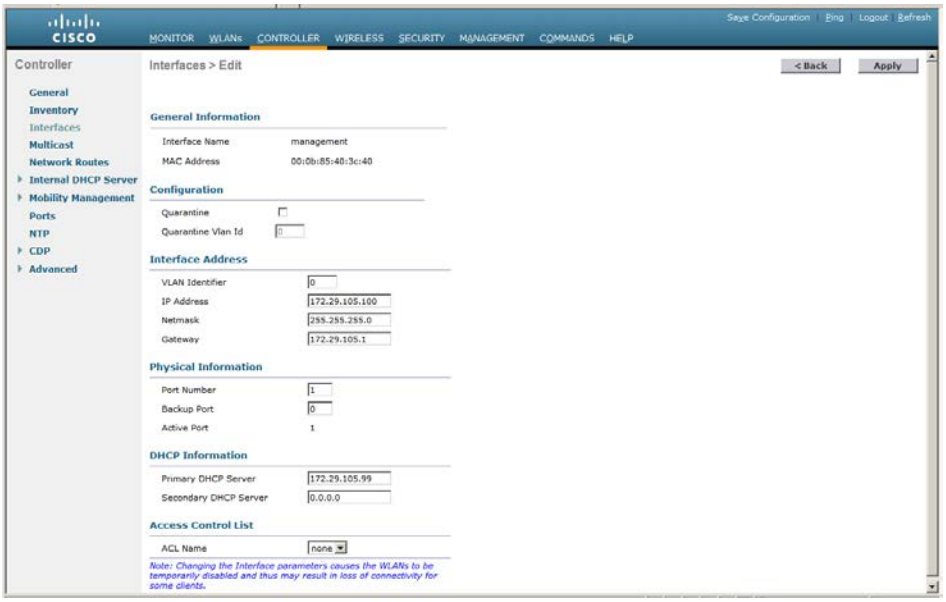
The **ap-manager** and **management** interfaces' configuration should include the DHCP server you have configured. Alternately, you can configure the DHCP server internally on the controller to hand out leases to the connected clients. (Note: The WLC's DHCP server does not lease addresses to the AP.) The instructions for doing so are included at the end of this document.

1. From the main menu, click **Controller**.
2. In the navigation pane, click **Interfaces**. Verify that the proper IP addresses are assigned to the interfaces.
3. Under Interface Name click **management**. Note: the screenshots are from a Cisco 4400. The 2100 does not contain a service-port interface. The 5500 does not contain an ap-manager interface. If the interface is not present on the model being configured, no values need to be entered.

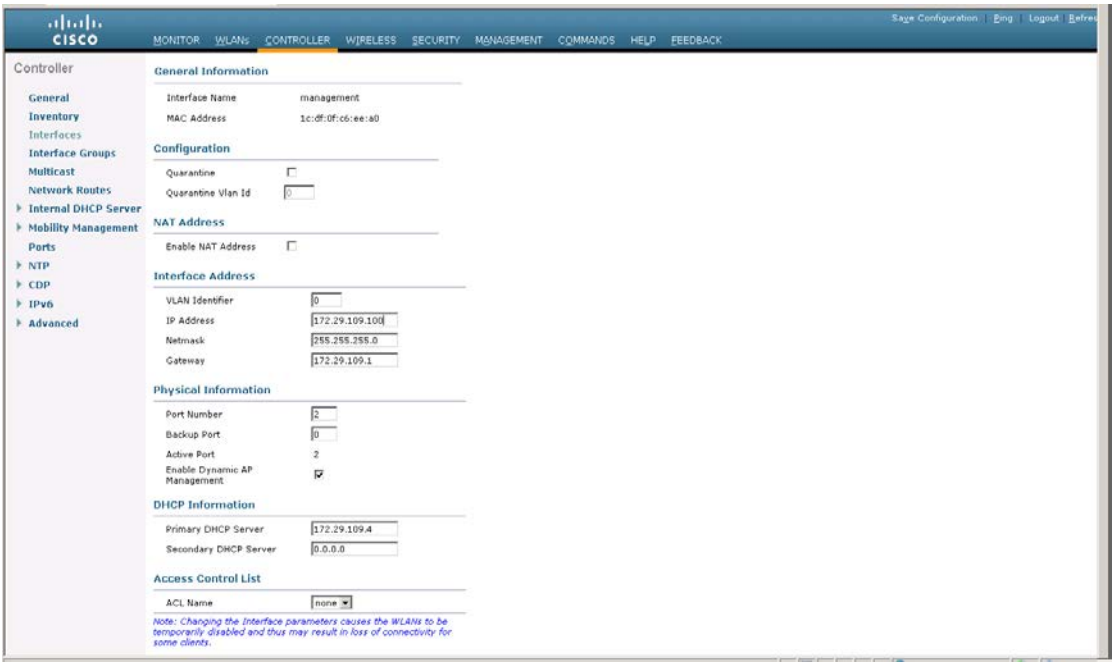


4. Under DHCP Information, enter the IP address of the Primary DHCP Server.
5. Repeat this step for the ap-manager interface, if present on the model configured.
6. Click the **Apply** button and save the changes.

Cisco Controllers other than the 5500:



Cisco 5500:

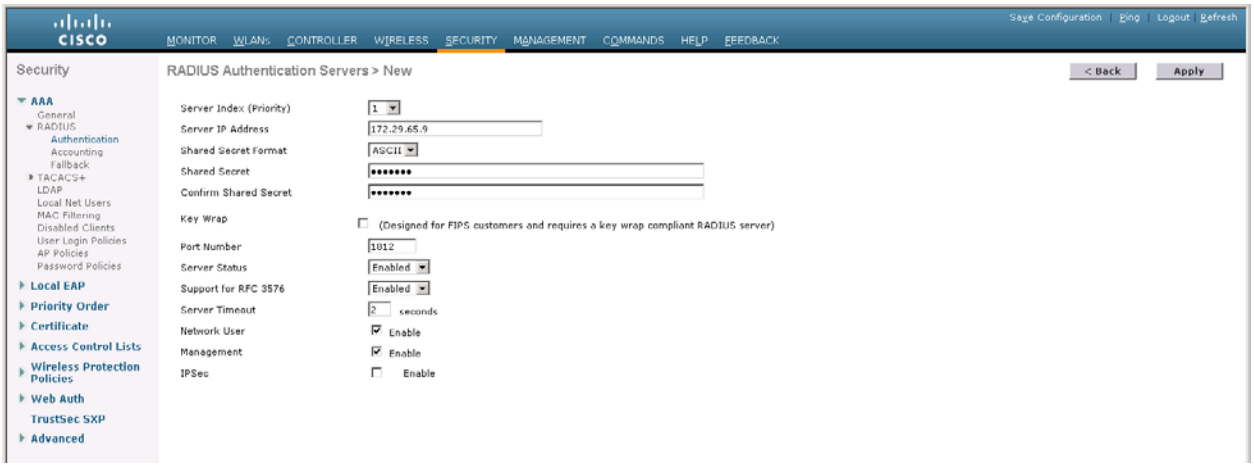


7 Under service-port, (if present), enter a valid IP Address and Netmask in a different subnet than the management interface. Click the **Apply** button and save the changes.

Defining a RADIUS Server

If it is desired to use WPA2-Enterprise security, it is necessary to define a RADIUS server.

1. From the main menu, click **SECURITY**.
2. Expand **RADIUS** in the left pane.
3. Click **Authentication**.
4. Click **New**… in the right hand corner of the screen.
5. Enter the IP Address of the RADIUS server in the Server IP Address field.
6. Enter the Shared Secret from the RADIUS server in the Shared Secret and Confirm Shared Secret fields.



7. Click **Apply**. The RADIUS server will now be available for selection in the WLANs menu security screens.

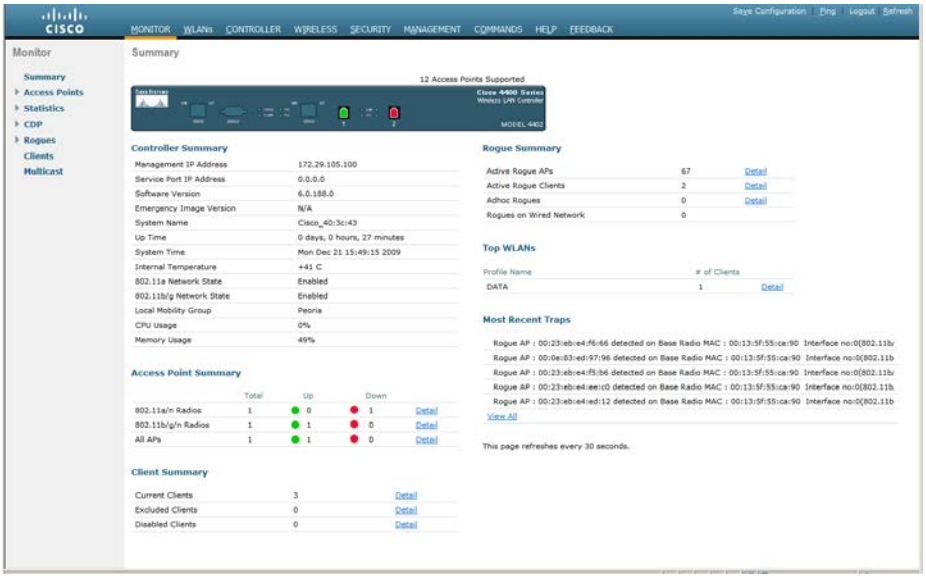
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec SXP
Advanced
RADIUS Authentication Servers
Apply
New...
Call Station ID Type 1
IP Address
Use AES Key Wrap
(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter
Hyphen
Network User
Management
Server Index
Server Address
Port
IPSec
Admin Status
1
172.29.65.9
1812
Disabled
Enabled
1. Call Station ID Type will be applicable only for non 802.1x authentication only.

AP Configuration

Settings: QoS setting

All handsets operating on a given AP radio must have the same QoS setting. All APs supporting the handsets must be configured to enable the corresponding features.

1. Power-on and connect the APs to the network. Wait a few minutes for the APs to find the controller.
2. Verify the APs are associated to the WLC.
3. From the main menu, click **Monitor**.

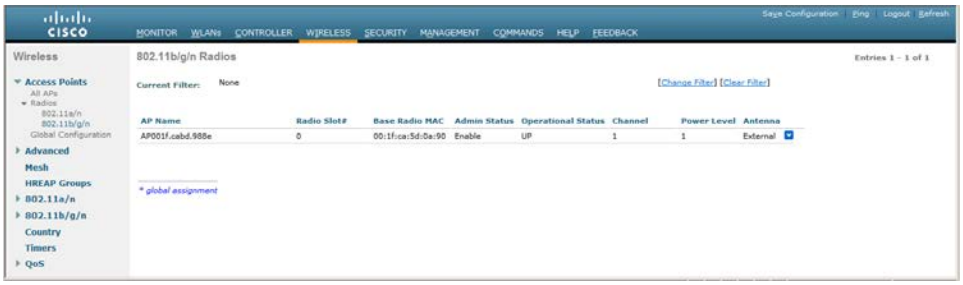


Configuration for handsets running in 802.11b & b/g mixed and g only mode

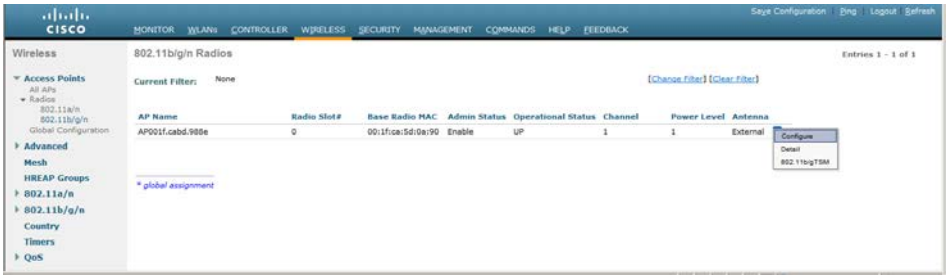
Admin Tip: When to use g-only

When 8020/8030 handsets are set to g only mode, they support the higher g data rates. In g only mode, however, the handset will not detect 802.11b clients and will not provide protection. G only mode in these handsets should be used only if there is no possibility of an 802.11b client or the network will experience data corruption.

1. From the main menu, click **Wireless**.
2. In the navigation pane, under Access Points click **Radios**, then select **802.11b/g/n**. All the APs that are connected should be listed, showing their Operational Status as UP.



3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:



Settings: Power and channel settings

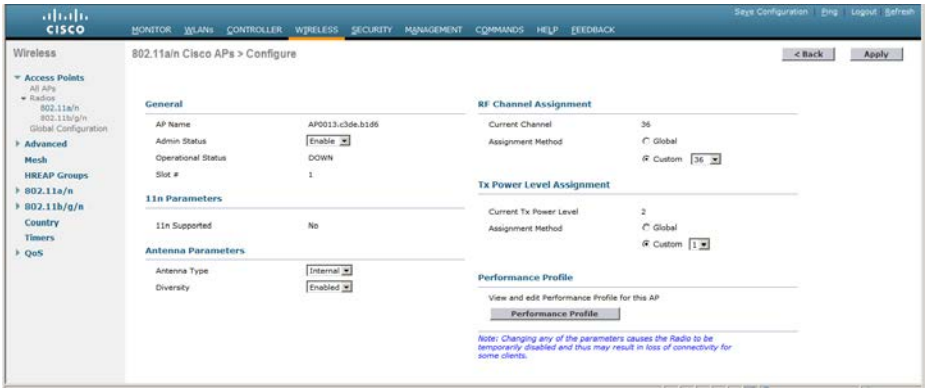
Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested. For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using only channels **1**, **6** and **11**.

a Set Admin Status to **Enable**.

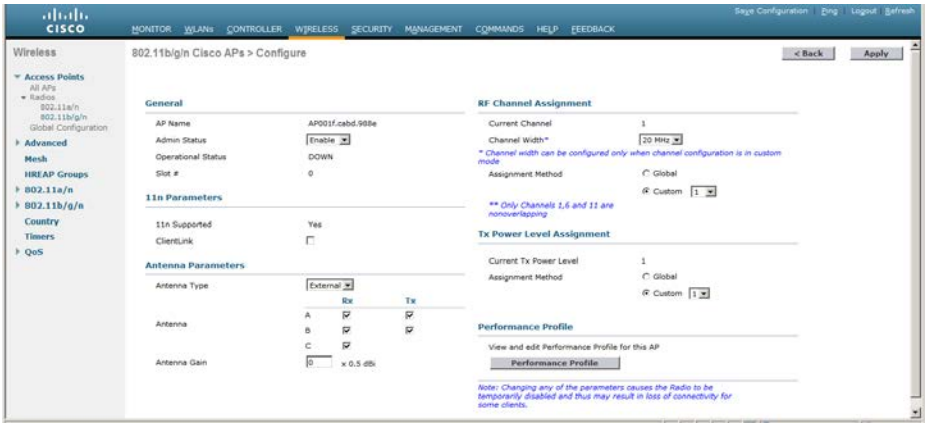
b Configure any other settings that might be relevant to your deployment as needed. In version 7.0.220.0, select only one antenna for transmission when using 80xx handsets. The CSD (cyclic shift diversity) algorithm has an incompatibility, which is not present in the other releases.

c Click the **Apply** button to save all changes.

Screenshot for access points with internal antennas:



Screenshot for access points with external antennas:



4 In the navigation pane under 802.11b/g/n, click **Network**. Set network parameters as follows:

a Set 802.11b/g Network Status to **Disable**. The radio will be re- enabled after setting radio parameters.

Settings: Data rates

For setting up the **Data Rates,** please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

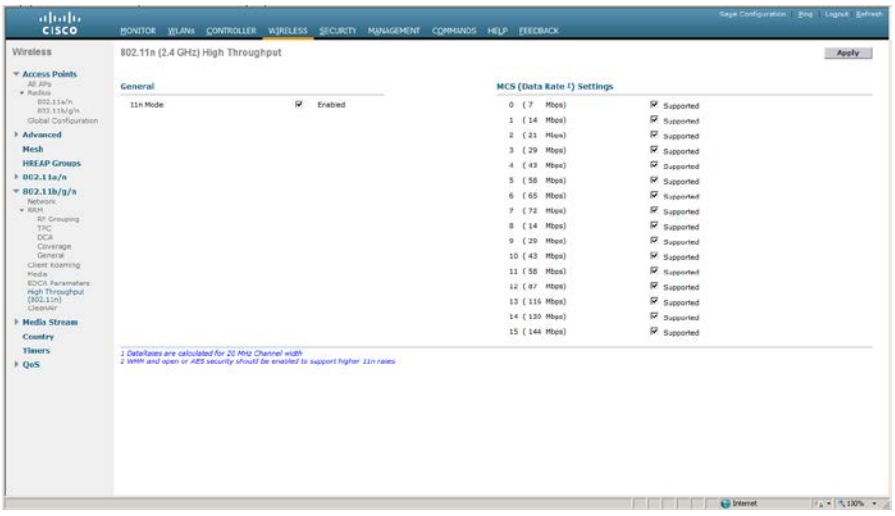
802.11 Radio Standard	*Minimum Available Signal Strength (RSSI)*	*Maximum "Mandatory" Data Rate*
802.11b	-75 dBm	1 Mb/s
	-65 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

Web Info: RF deployment

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide to Network Design Considerations for Spectralink Wireless Telephones*.

Configuring 802.11n

1 In the navigation pane under 802.11 b/g/n, select **High Throughput** (802.11n). Check the radio box to enable **11n** mode and allow all data rates to be supported.



2 **Disable** msdu aggregation:

a Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.

b Enter the commands:

```
config 802.11b 11nsupport a-msdu tx priority all disable
save config
```

3 If an 1142 ap is in use, disable mpdu aggregation.

a Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.

b Enter the commands:

```
config 802.11b 11nsupport a-mpdu tx priority all disable
save config
```

4 Click the **Apply** button to save the settings.

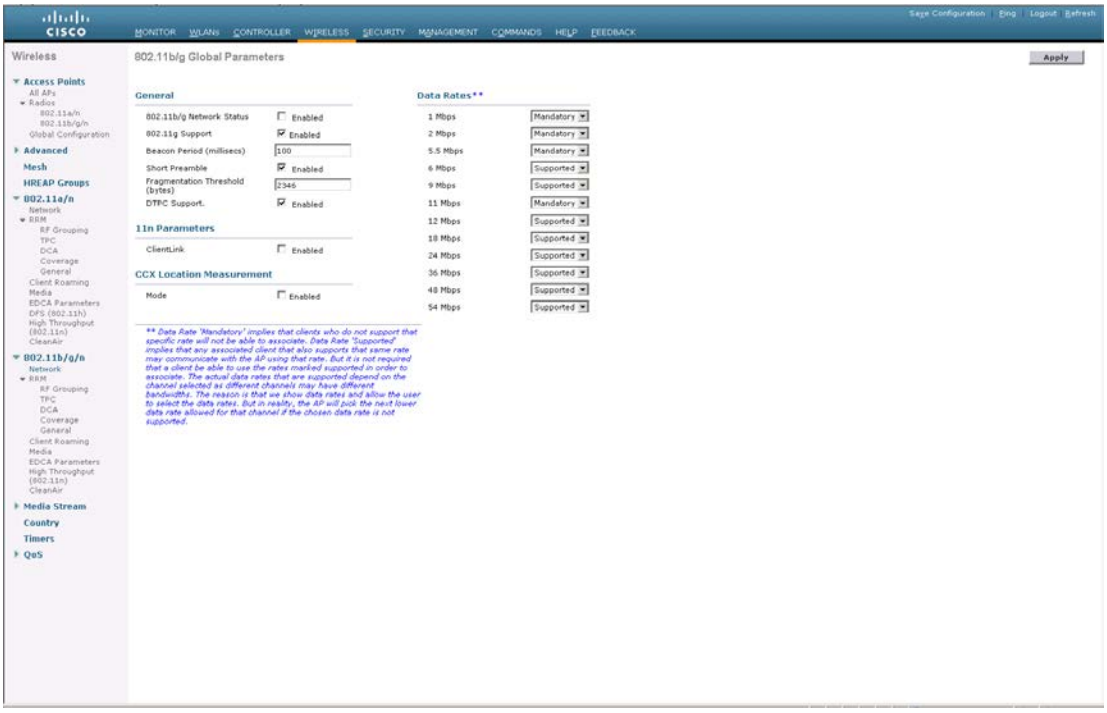
5 In the navigation pane under 802.11b/g/n, select **Network**.

6 For 802.11b/g Network Status, click the **Enabled** check box.

a Use the default Fragmentation Threshold (2346 bytes).

b Set the Beacon Period to 100.

c Click the **Apply** button to save the settings.

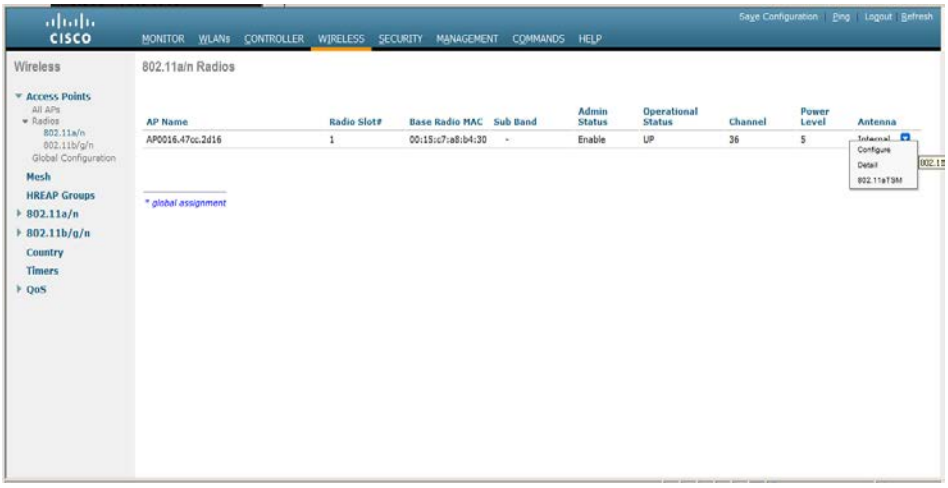


Configuration for handsets running in 802.11a mode

1 From the main menu, click **Wireless**.

2 In the navigation pane, under Access Points click **Radios**, then select **802.11a /n**. All the APs that are connected should be listed, showing their Operational Status as **UP**.

3 Select **Configure** from the drop-down list for the access point you wish to change. Set the parameters for that AP:



Settings: Power and channel settings

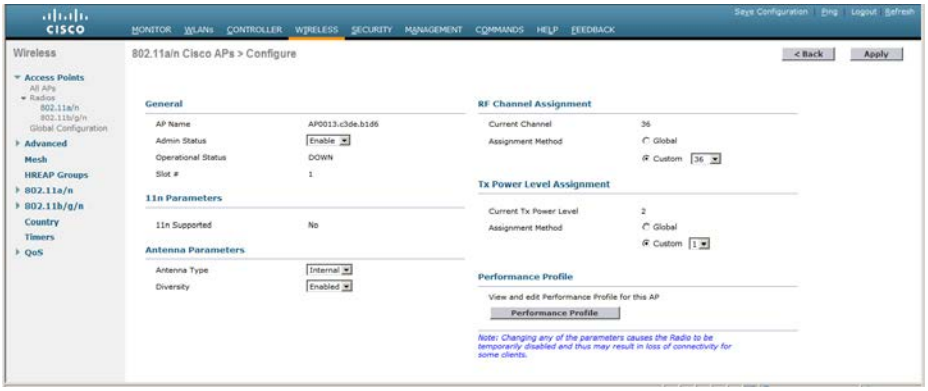
Global settings for **RF Channel Assignment** and **Tx Power Level Assignment** were not tested. For **Custom Tx Power** and **RF Channel** settings please consult your facility's RF site survey — optimized for wireless voice traffic — to determine correct power and channel settings for each AP using non-overlapping channels.

a Set Admin Status to **Enable**.

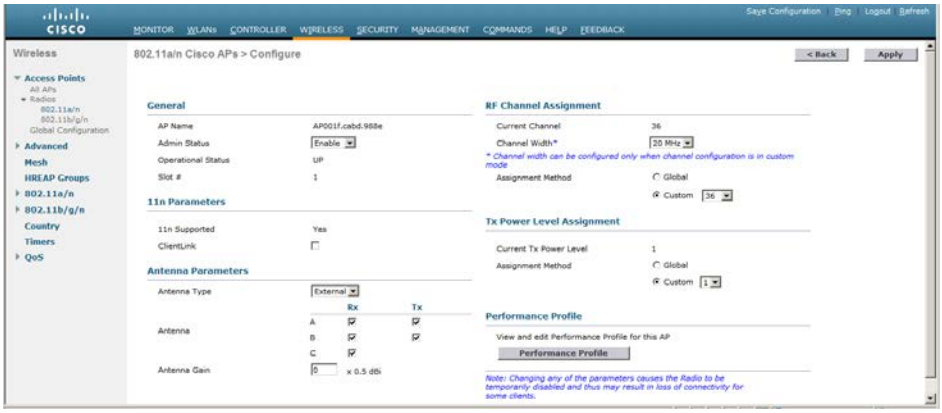
b Configure any other settings that might be relevant to your deployment as needed.

c Click the **Apply** button to save all changes.

Screenshot for access points with internal antennas:



Screenshot for access points with external antennas:



4 In the navigation pane under 802.11a/n, click **Network**. Set the network parameters as follows:

a Set 802.11a Network Status to **Disable**; the radio will be re-enabled after setting radio parameters

b For setting up the Data Rates, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. The handset requires the following minimum dBm reading to support the corresponding Mandatory data rate setting in the access point.

802.11 Radio Standard	*Minimum Available Signal Strength (RSSI)*	*Maximum "Mandatory" Data Rate*
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

Web Info: RF deployment reference

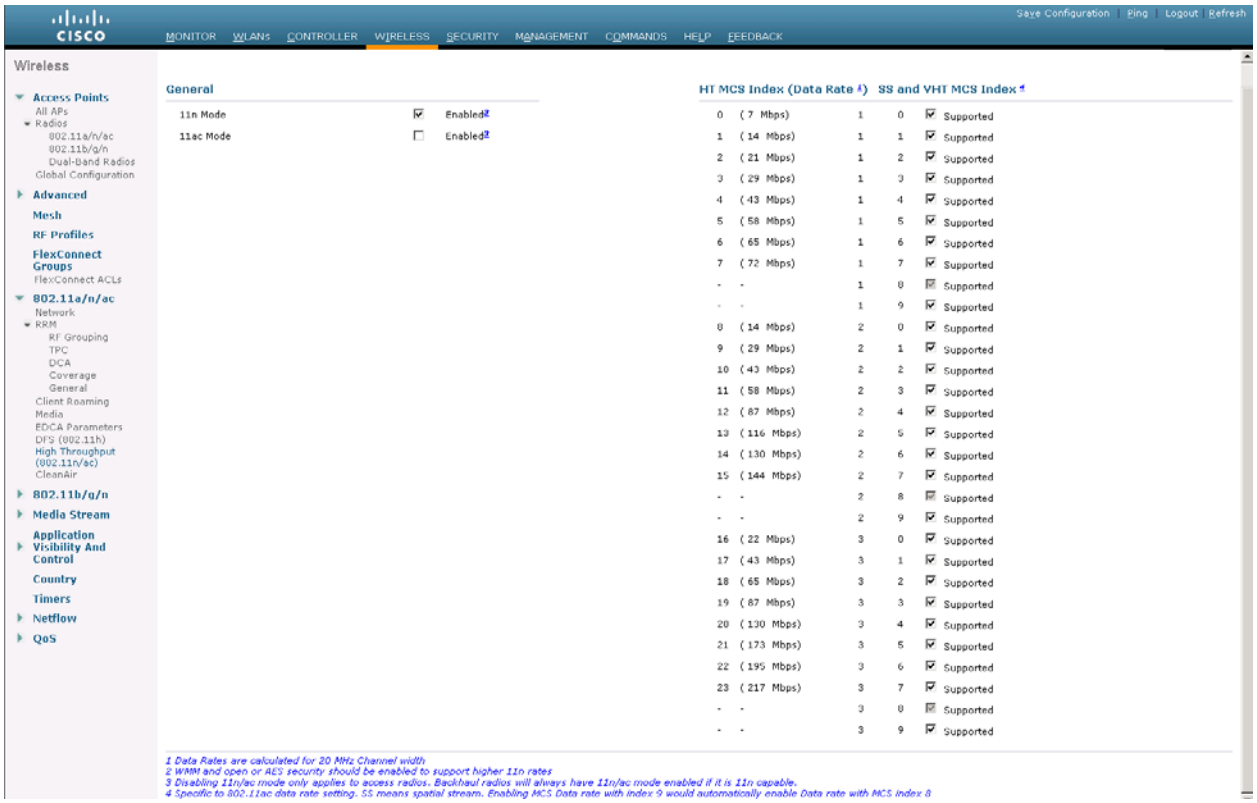
For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* white paper and the *Best Practices Guide to Network Design Considerations for Spectralink Wireless Telephone*.

Configuring 802.11n:

1 In the navigation pane under 802.11 a/n, select **High Throughput** (**802.11n**). Check the radio box to enable 11n mode and allow all data rates to be supported.

802.11a/n AP's

802.11a/n/ac AP's



Admin Tip: 802.11ac

Spectralink has not yet been tested with 802.11ac clients in the network. It is known that the handsets operate properly with 802.11ac turned off as shown.

2 **Disable** msdu aggregation:

a Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.

b Enter the commands:

```
config 802.11a 11nsupport a-msdu tx priority all disable
save config
```

3 If an 1142 ap is in use, disable mpdu aggregation.

a Connect to the CLI as described in the section “Configuring a New Controller Starting from Factory Defaults”.

b Enter the commands:

```
config 802.11a 11nsupport a-mpdu tx priority all disable
save config
```

4 In the navigation pane under 802.11a/n, select **Network**.

5 For 802.11a Network Status, click the **Enabled** check box.

6 Click the **Apply** button to save the settings.

Setting up the SSID

Voice and data must be on separate SSIDs to prioritize voice traffic. The voice SSID must be set to **Platinum** for **Quality of Service** and the data SSID must be set to **Silver** for **Quality of Service**.

1. From the main menu, click **WLANs**.
2. In the WLANs screen, select **Create New** from the drop down list and click **Go**.

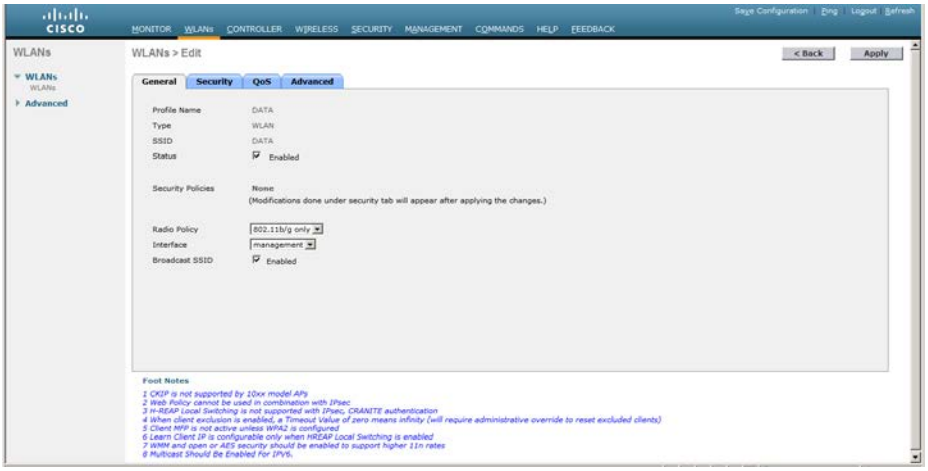
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
WLANs
Advanced
Entries 0 - 0 of 0
Current Filter: None [Change Filter] [Clear Filter]
Create New
Go
WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

3. Enter the Profile Name and SSID.
4. Click the **Apply** button twice.

Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
WLANs
Advanced
Entries 1 - 2 of 2
Current Filter: None [Change Filter] [Clear Filter]
Create New
Go
WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies
1 WLAN Voice 101V Disabled [WPA2][Auth(802.1X)]
2 WLAN Data 101D Disabled [WPA2][Auth(802.1X)]

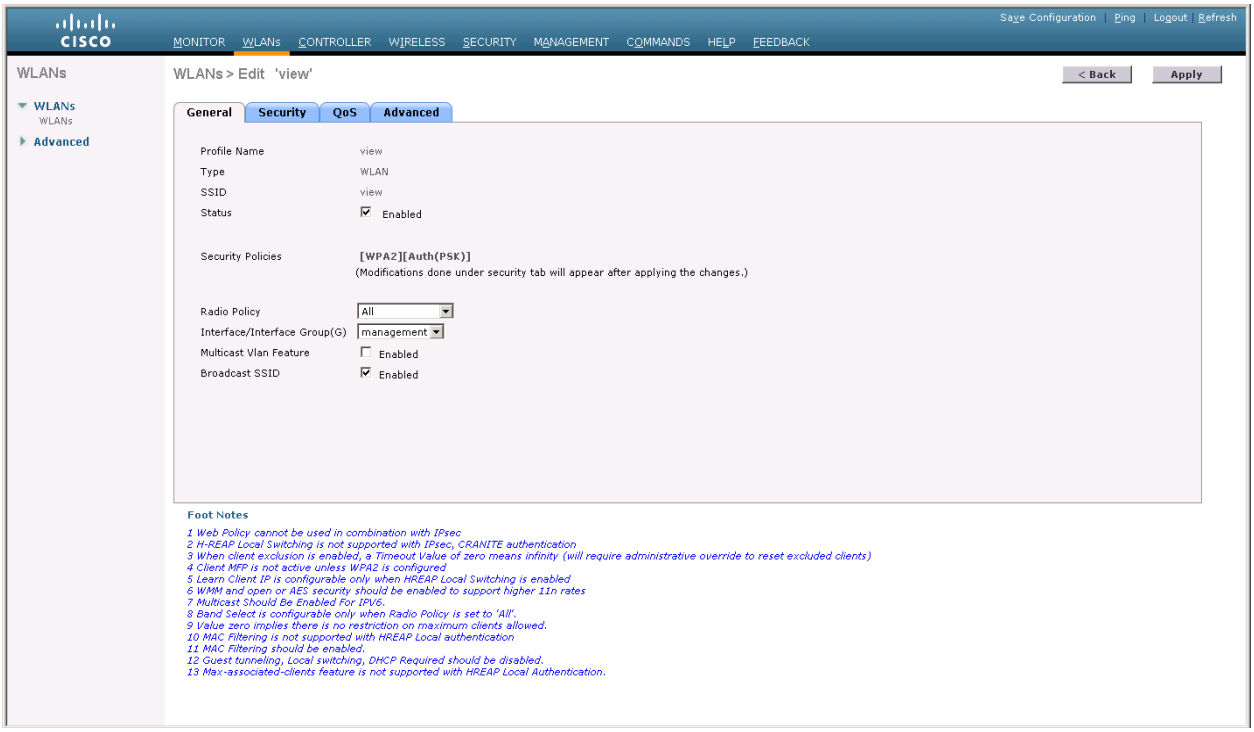
5. Select the Profile Name for the voice SSID.
6. Under the General tab, verify the Radio Policy corresponds to the Spectralink Wireless Telephone configuration.
   - When Radio Policy is configured for 802.11b/g only, the handsets should be configured for 802.11b & b/g mixed in 8020/8030
   - When Radio Policy is configured for 802.11a only, the handsets should be configured for 802.11a in 8020/8030 handsets.
   - When Radio Policy is configured for 802.11g only, the handsets should be configured for 802.11g only in 8020/8030.
   - When Radio Policy is configured for All, the handsets may be configured to any of the settings required.
7. For Status, select the **Enabled** check box.

Cisco 6.0 Versions:



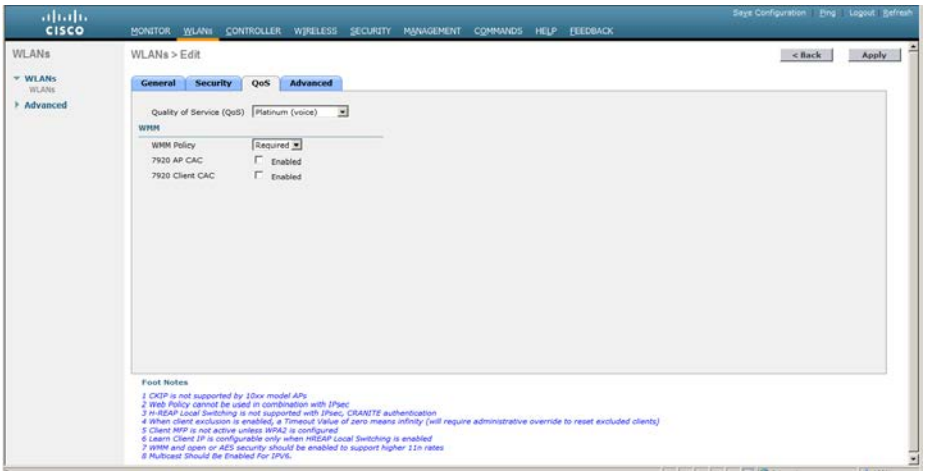
Other versions:

(Ensure that the Multicast Vlan Feature remains unchecked for proper PTT performance.)


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs > Edit 'view'
< Back
Apply
General
Security
QoS
Advanced
Profile Name
view
Type
WLAN
SSID
view
Status
Enabled
Security Policies
[WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G)
management
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
Foot Notes
1 Web Policy cannot be used in combination with IPsec
2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when HREAP Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Multicast Should Be Enabled For IPV6.
8 Band Select is configurable only when Radio Policy is set to 'All'.
9 Value zero implies there is no restriction on maximum clients allowed.
10 MAC Filtering is not supported with HREAP Local authentication
11 MAC Filtering should be enabled.
12 Guest tunneling, Local switching, DHCP Required should be disabled.
13 Max-associated-clients feature is not supported with HREAP Local Authentication.

8 Under the QoS tab, set Quality of Service to **Platinum**. This is the required setting for voice traffic.

9 Set WMM Policy to **Disabled**.

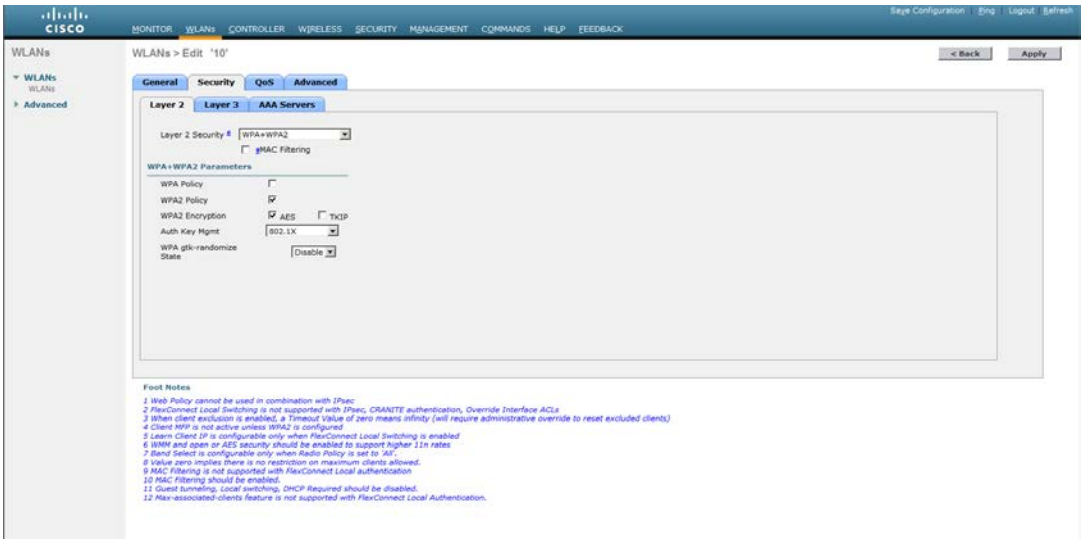


10 Under the Security tab, at Layer 2 Security select the desired security policy from the drop-down list.

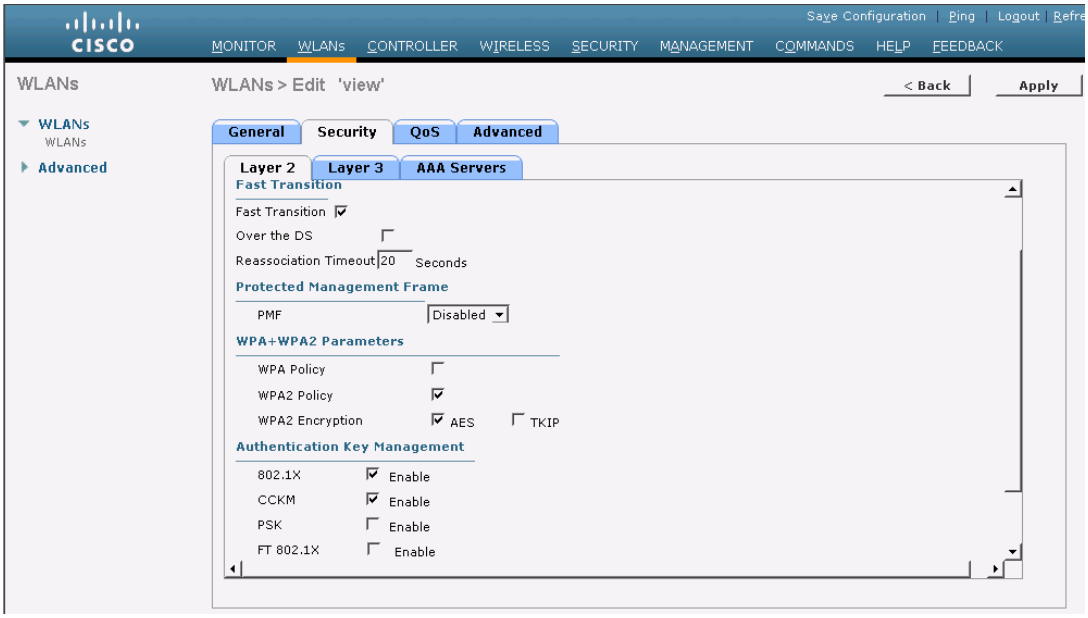
- For WPA2-PSK, under WPA+WPA2 Parameters:
  - **i** Select the **WPA2-Policy** check box.
  - **ii** Select the **AES** check box for **WPA2-Encryption**.
  - **iii** At **Auth Key Mgmt** select **PSK** from the drop-down list.
  - **iv** If present (7.2. and later versions), ensure that **WPA gtk-randomize State** is set to **Disable**. The Fast Transition and FT PSK radio boxes may be checked or unchecked as desired.
- For WPA-PSK, under WPA+WPA2 Parameters:
  - **i** Select the WPA-Policy check box.
  - **ii** Select the TKIP check box for WPA Encryption.
  - **iii** At Auth Key Mgmt select PSK from the drop-down list. The PSK Format may be selected as ASCII or HEX for both WPA-PSK and WPA2-PSK policies.
  - **iv** If present (7.2 and later versions), ensure that the Fast Transition and FT boxes remain unchecked.
  - **v** If present (7.2. and later versions), ensure that WPA gtk-randomize State is set to Disable. The Fast Transition and FT PSK radio boxes may be checked or unchecked as desired.
- For WPA2-Enterprise (802.1X), select WPA+WPA2 Parameters:
  - **i** Select the **WPA2 Policy** check box.
  - **ii** Select the **AES** check box for **WPA2 Encryption**.
  - **iii** At **Auth Key Mgmt**, select **802.1X+CCKM** from the drop-down list.
  - **iv** If present (7.2. and later versions), ensure that **WPA gtk-randomize State** is set to **Disable**.

- **v** If present (7.2 and later versions), the **Fast Transition** radio box may be checked to permit other devices to use 802.11r but the **FT 802.1x** radio box must not be checked as it limits network access to 802.11r devices only.

Cisco 6.0 and 7.0 Versions:



Cisco 7.2 and later Versions:



11 Under the Advanced tab

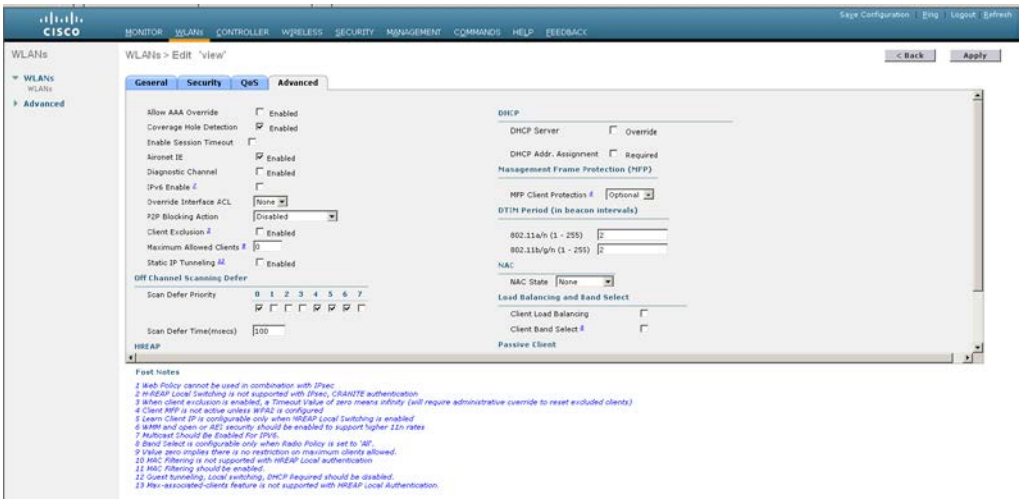
- **a** Set the DTIM to **2** for the radio that corresponds to the Spectralink Wireless handset configuration.

b Ensure the Enable Session Timeout box is unchecked and that Client Exclusion is disabled.

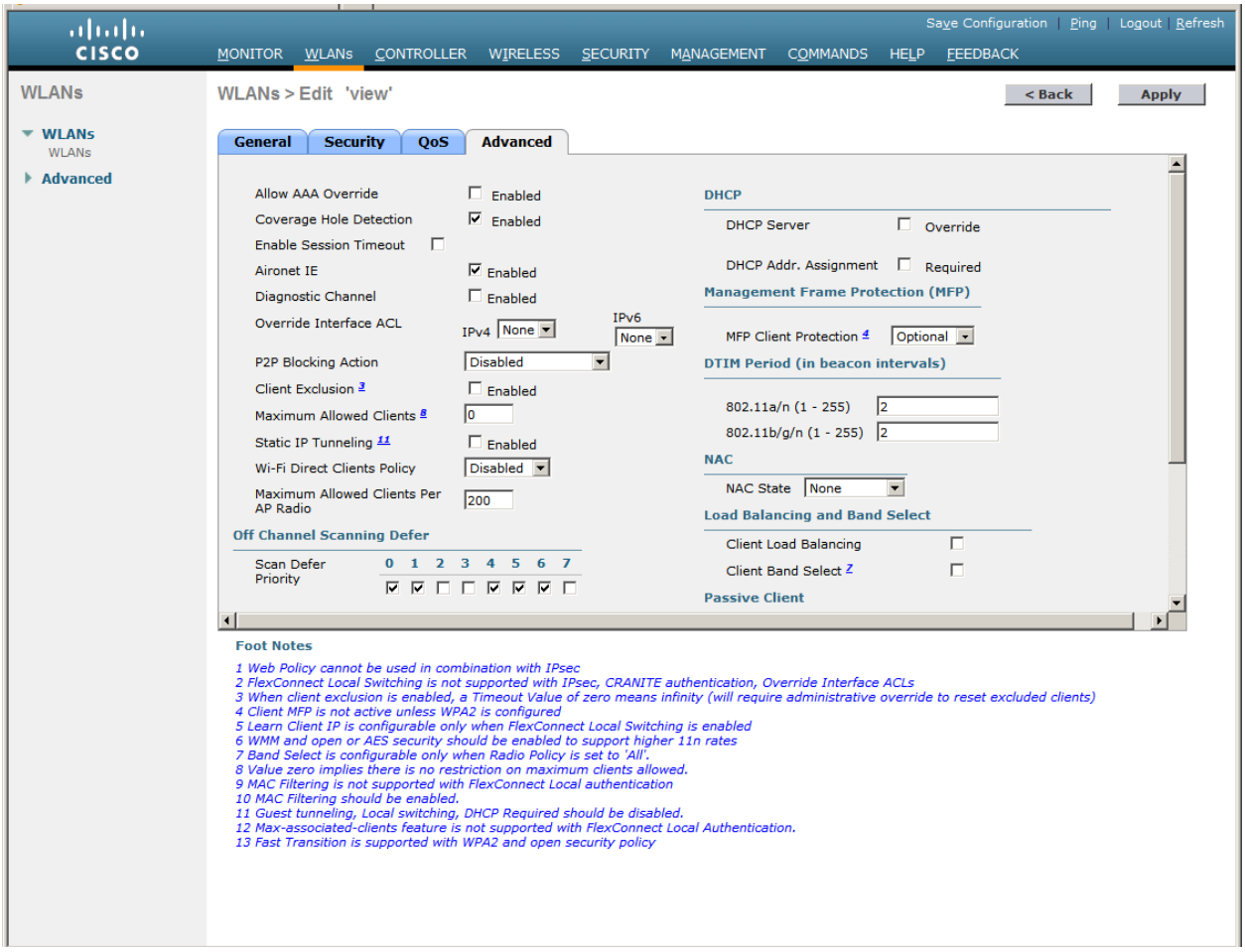
c Uncheck the Client Load Balancing and Client Band Select boxes.

d Check off-channel scanning defer for the 0 priority class (prevents contention between off-channel scanning and PTT).

Cisco 6.0 and 7.0 versions:



Cisco 7.2 and later versions:


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'view'
< Back
Apply
General
Security
QoS
Advanced
Allow AAA Override
Enabled
Coverage Hole Detection
Enabled
Enable Session Timeout
Aironet IE
Enabled
Diagnostic Channel
Enabled
Override Interface ACL
IPv4 None
IPv6 None
P2P Blocking Action
Disabled
Client Exclusion 3
Enabled
Maximum Allowed Clients 8
0
Static IP Tunneling 11
Enabled
Wi-Fi Direct Clients Policy
Disabled
Maximum Allowed Clients Per AP Radio
200
Off Channel Scanning Defer
Scan Defer Priority
0 1 2 3 4 5 6 7
DHCP
DHCP Server
Override
DHCP Addr. Assignment
Required
Management Frame Protection (MFP)
MFP Client Protection 4
Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255)
2
802.11b/g/n (1 - 255)
2
NAC
NAC State
None
Load Balancing and Band Select
Client Load Balancing
Client Band Select 7
Passive Client
Foot Notes
1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.
13 Fast Transition is supported with WPA2 and open security policy

12 Click the **Apply** button to save all changes.

Setting up the EDCA parameters profile

The EDCA parameters must be set to the WMM setting after the WLAN network QoS has been set.

Configuration for handsets running in 802.11a mode mode in 8020/8030 handsets

1. In the navigation pane under 802.11a/n, select **EDCA Parameters**.
2. Ensure that **Spectralink Voice Priority** is selected from the drop-down list.
3. Click **Apply**.

Configuration for handsets running in 802.11b/g mode, 802.11b and b/g mixed mode, or 802.11 g only mode in 8020/8030 handsets

1. In the navigation pane under 802.11b/g/n, select **EDCA Parameters**.
2. Select **Spectralink Voice Priority** from the drop-down list.
3. Click the **Apply** button to save the settings.

Settings: SVP and 802.11n

When Spectralink Voice Priority (SVP) is enabled under the EDCA parameters setting, the 802.11n capabilities will be disabled on that radio on Cisco 6.0 version releases. Spectralink recommends deploying handsets using SVP on a different radio than 802.11n clients for Cisco 6.0 version releases.